NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

REMEDIATING THIRD-PARTY SOFTWARE VULNERABILITIES ON U.S. ARMY INFORMATION SYSTEMS

by

Jason R. Sabovich
James A. Borst

June 2012

Thesis Advisor:	Raymond R. Buettner
Second Reader:	Albert Barreto
Third Reader:	Glenn Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Remediating Third-Party Software Vulnerabilities on U.S. Army Information Systems		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Jason R. Sabovich and James A. Borst			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Information systems belonging to the DoD and U.S. Army experience cyber attacks on a daily basis. Increasingly, these attacks are targeting popular third-party applications, instead of focusing on vulnerabilities in Microsoft software. The DoD responded to this threat by adopting Citadel Hercules, which did not find a willing audience with the U.S. Army. Instead, the Army adopted Microsoft Systems Management Server (SMS), followed by System Center Configuration Manager (SCCM) 2007 to meet this threat. After more than five years, the rollout of SCCM to all organizations within the U.S. Army is still incomplete. This study provides an overview of the threats facing U.S. Army information systems and looks at how the Army has addressed this challenge in the past. Next, the study takes a system engineering approach to identifying an optimal tool for mitigating third-party vulnerabilities and suggests potential alternatives to SCCM. In addition, the study utilizes a cost benefit analysis approach to aid in evaluating the potential Return on Investment (ROI) provided by each tool. The purpose of this study is to answer the question: What is the most optimal solution for mitigating vulnerabilities in third-party applications on U.S. Army information systems?

14. SUBJECT TERMS Information Assurance Vulnerability Message (IAVM), Patch Management, Third-Party Vulnerability Remediation, System Center Configuration Manager (SCCM), LandWarNet (LWN), Information Assurance Vulnerability Alert (IAVA), Network Operations and Security Center (NOSC), Patching, SysMan			**15. NUMBER OF PAGES** 167
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

REMEDIATING THIRD-PARTY SOFTWARE VULNERABILITIES ON U.S. ARMY INFORMATION SYSTEMS

Jason R. Sabovich
Major, United States Army
B.S., California Polytechnic State University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

James A. Borst
Major, United States Army
B.A., Saint Martin's University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2012

Authors: Jason R. Sabovich

James A. Borst

Approved by: Raymond R. Buettner
Thesis Advisor

Albert Barreto
Second Reader

Glenn Cook
Third Reader

Dan Boger
Chair, Department of Information Sciences

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Information systems belonging to the DoD and U.S. Army experience cyber attacks on a daily basis. Increasingly, these attacks are targeting popular third-party applications, instead of focusing on vulnerabilities in Microsoft software. The DoD responded to this threat by adopting Citadel Hercules, which did not find a willing audience with the U.S. Army. Instead, the Army adopted Microsoft Systems Management Server (SMS), followed by System Center Configuration Manager (SCCM) 2007 to meet this threat. After more than five years, the rollout of SCCM to all organizations within the U.S. Army is still incomplete. This study provides an overview of the threats facing U.S. Army information systems and looks at how the Army has addressed this challenge in the past. Next, the study takes a system engineering approach to identifying an optimal tool for mitigating third-party vulnerabilities and suggests potential alternatives to SCCM. In addition, the study utilizes a cost benefit analysis approach to aid in evaluating the potential Return on Investment (ROI) provided by each tool. The purpose of this study is to answer the question: What is the most optimal solution for mitigating vulnerabilities in third-party applications on U.S. Army information systems?

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AKO	Army Knowledge Online
ARCYBER	Army Cyber Command
BCCS	Battle Command Common Services
BCT	Brigade Combat Team
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CHESS	Computer Hardware Enterprise Software and Solutions
CM	Configuration Management
CNA	Computer Network Attack
CNO	Computer Network Operations
COA	Course of Action
CVE	Collaborative Virtual Environment
DHCP	Dynamic Host Configuration Protocol
DoD	Department of Defense
DoS	Denial of Service
DMZ	Demilitarized Zone
DNS	Domain Name System
EW	Electronic Warfare
FOB	Forward Operating Base
G6	Communications Officer (Brigade or above level)
GIG	Global Information Grid
GNEC	Global Network Enterprise Construct
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IO	Information Operations
IMO	Information Management Officer
IW	Information Warfare
JNN	Joint Network Node
JP	Joint Publication
LAN	Local Area Network
LCC	Life-Cycle Costing
LWN	Land War Network

MDM	Mobile Device Management
MILDEC	Military Deception
NCIJTF	National Cyber Investigative Joint Task Force
NEC	Network Enterprise Center
NETCOM	Network Enterprise Technology Command
NIPP	National Infrastructure Protection Plan
NIPR	Non-Classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NOSC	Network Operations and Security Center
NVD	National Vulnerability Database
OMB	Office of Management and Budget
OPSEC	Operational Security
PSYOP	Psychological Operations
QMX	Quest Xtensions Manager
RCERT	Regional Computer Emergency Response Team
REM	Remote Enterprise Manager
S6	Communications Officer (Battalion Level)
SATCOM	Satellite Communications
SCCM	System Center Configuration Manager
SCOM	System Center Operations Manager
SCRI	Secure Configuration Remediation Initiative
SCUP	System Center Update Publisher
SIPR	Secret Internet Protocol Router Network
SysMan	Systems Manager
TNOSC	Theater Network Operations Security Center
TTP	Tactics, Techniques, and Procedures
USCERT	United States Computer Emergency Readiness Team
USDHS	United States Department of Homeland Security
VoIP	Voice over IP
VTC	Video Tele-Conference
WAN	Wide Area Network
WGS	Wideband Global Satellite
WIN-T	Warfighter Information Network—Tomorrow
WSUS	Windows Server Update Services

ACKNOWLEDGMENTS

Jason: I would like to thank my wife, Christina Sabovich, for watching our three girls while I locked myself away in the office working on this thesis. Thank you for the editing, advice, and support you provided during this difficult process. I could not have done it without you.

Additionally I would also like to thank Dr. Raymond Buettner, Mr. Albert Barreto and Mr. Glen Cook. You each provided a great deal of help when I needed it. Thank you for taking the time out of your busy schedules to mentor me. I would also like to thank my Navy, Air Force, Army and Marine colleagues at NPS. Your support helped to keep me on track with this thesis.

James: I would like to thank Jason for graciously allowing me to work with him on this thesis to provide a business perspective in addition to the more technical knowledge he brought to the table. I would also like to thank my wife, Amy and three kids for putting up with my noticeable absences on days I did not have class, but spent at the library working instead. Your endless love and selfless support and encouragement this past year and a half, was in the end, what made this possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Cyber attacks against the Department of Defense's (DoD) Global Information Grid (GIG) occur by the thousands on a daily basis.[1] Between September 2008 and March 2009, the DoD reported spending over $100 million to repair damages resulting from cyber attacks.[2] Unlike conventional attacks, cyber attacks can be conducted cheaply and often with anonymity. To meet this challenge, the GIG employs a defense in-depth strategy under the control of U.S. Cyber Command (USCYBERCOM) based out of Fort Meade, MD. On September 7, 2010, USCYBERCOM relieved the Joint Task Force-Global Network Operations (JTF-GNO) of its mission to operate and defend the GIG in both times of peace and war.[3] Each of the services operates a subordinate command to USCYBERCOM with the responsibility of defending their portion of the GIG. Defense of the GIG also falls within the functional area of Information Operations (IO). IO exists to provide joint commanders with a decisive information advantage, while denying or controlling the information that enemy commanders need to make sound decisions, which is the domain of Computer Network Operations (CNO), which includes Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defense (CND).[4] The goal of CND is to secure DoD networks, as well as the information systems operating within networks from attack by sources both internal and external to the DoD.[5] Within the U.S. Army, it is the mission of Army Cyber Command (ARCYBER) to defend the Army's portion of the GIG, known as the LandWarNet (LWN).

---

[1] CBS Interactive Staff, "DoD Gates: We're Always Under Cyberattack," *ZDNet*, April 22, 2009, http://www.zdnet.com/news/dod-gates-were-always-under-cyberattack/290770.

[2] Elinor Mills, "Pentagon Spends Over $100 Million on Cyberattack Cleanup," *CNET News*, April 7, 2009, http://news.cnet.com/8301-1009_3-10214416-83.html.

[3] Michael J. Carden, "Cyber Task Force Passes Mission to Cyber Command," *American Forces Press Service*, September 8, 2010, http://www.af.mil/news/story.asp?id=123221046.

[4] Headquarters, Department of the Army, "FM 3-13, Information Operations: Doctrine, Tactics, Techniques, and Procedures," U.S. Army Training and Doctrine Command, 2003, https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fm3_13.pdf, iii–v.

[5] P. A. Snyder, "The Department of Defense Must Combat Terrorism with Cyber Attacks," *Defense Technical Information Center*, October 20, 2008, http://handle.dtic.mil/100.2/ADA500190.

Experts have long warned that no network is completely secure, and the LWN is no exception.[6] The Army segments the LWN into four parts, including the Global Defense Network, the Post/Camp/Station Network, the At Home/TDY Network, and the Deployed Tactical Network as shown in Figure 1.[7]

Figure 1. The Army Enterprise Network (LandWarNet)[8]

Each of these networks presents unique challenges to network security. Given the potential of adversaries to penetrate U.S. networks, the U.S. Army must secure its information systems to the greatest extent possible, while still allowing them to complete the functions for which they were intended. Keeping information systems securely patched by installing vendor supplied updates is an effective means of diminishing the

[6] Anthony Bellissimo, John Burgess, and Kevin Fu, "Secure Software Updates: Disappointments and New Challenges," Proceedings of the 1st USENIX Workshop on Hot Topics in Security, *USENIX Association*, 2006, http://static.usenix.org/event/hotsec06/tech/full_papers/bellissimo/bellissimo.pdf.

[7] Army CIO G6, "Common Operating Environment Architecture: Appendix C to Guidance for 'End State' Army Enterprise Network Architecture," *Army Chief Information Officer G-6*, October 1, 2010, http://ciog6.army.mil/LinkClick.aspx?fileticket=udbujAHXmK0%3D&tabid=79, 5.

[8] Ibid.

threat of known exploits. Of successful network attacks, nearly 95% could have been prevented if current patches had been installed.[9] Of course, this percentage is only what has been reported. Many experts think that the majority of cyber crimes actually go unreported because victims of cyber crime are unaware they even occurred.[10] Unfortunately, keeping information systems properly updated has proven to be a monumental task for most organizations, including the U.S. Army.

Along with commercial organizations, the U.S. Army made the switch to personal computers in the early 1990s, and selected Microsoft Windows as its operating system of choice. In 1994, Microsoft introduced Systems Management Server (SMS), which provided the capability for organizations to deploy software packages, including operating systems, such as Windows 95.[11] The release of Windows 95 coincided with the public launch of the Windows Update website. Unfortunately, this update capability was available only as a direct service from Microsoft, which prevented organizations from controlling the updating process on their corporate PCs. During this time, cyber criminals were quick to target Windows vulnerabilities because most organizations had not deployed automated patching tools. Microsoft SMS was not widely used, as it was expensive and complex to deploy and operate. Most system administrators patched PCs and deployed software packages manually. In early 2003, to address this problem and complement SMS 2003, Microsoft released Software Update Services (SUS), free of charge.[12] SUS servers in an organization had the capability to deploy critical operating system updates prepackaged from Microsoft. SUS essentially allowed an organization to manage its own internal Windows Update servers. The low cost, simplicity and effectiveness of SUS resulted in widespread acceptance and adoption throughout

---

[9] Michael Czumak III, "Recommendations for a Standardized Program Management Office (PMO) Time Compliance Network Order (TCNO) Patching Process," (master's thesis, Air Force Institute of Technology, 2007).

[10] CERT, "2010 Cyber Security Watch Survey: Cybercrime Increasing Faster Than Some Company Defenses," January 25, 2010, http://www.cert.org/archive/pdf/ecrimesummary10.pdf.

[11] Microsoft, "Systems Management Server," *Microsoft TechNet*, (n.d.), http://technet.microsoft.com/en-us/library/cc723685.aspx.

[12] Mandy Andress, "Windows Patch Management Tools," *Network World*, 2003, http://books.google.com/books?id=YxkEAAAAMBAJ&pg=PT37&dq=microsoft+sus+released&hl=en&sa=X&ei=CdFGT-e8O-bSiAL42ITbDQ&sqi=2#v=onepage&q=microsoft%20sus%20released&f=false, 38.

corporate America and the DoD. Unfortunately, SUS was not a complete solution because it only supported critical Windows OS updates. Recognizing this limitation, SUS was upgraded by Microsoft in 2005 and became known as Windows Server Update Services (WSUS). WSUS added increased functionality, including support for Windows Server operating systems, Microsoft Office and other Microsoft products. Unfortunately, WSUS failed to address third-party application vulnerabilities. Other vendors, such as BigFix, Shavlik, Patchlink, and others responded by offering their own patching solutions for both Microsoft and third-party applications.[13]

In 2007, Microsoft upgraded SMS to System Center Configuration Manager 2007 (SCCM), which, among other improvements, allowed SCCM to control WSUS servers using a single interface on SCCM. As Microsoft products became more secure due to automated updating, cyber criminals shifted their focus and their attacks to third-party applications unprotected by SUS/WSUS. The Army was slow to respond to the increased threat to third-party applications. The third-party application vulnerability threat represented a serious challenge not being addressed by a single vendor, as Microsoft had done with the WSUS because each third-party vendor specified its own update mechanism. At the same time, Army information systems were experiencing a large increase in the number of third-party applications approved for operation on the network. In response to this problem, the DoD Enterprise-wide IA & CND Solutions Steering Group (ESSG) selected Citadel Hercules as the DoD vulnerability remediation tool of choice in 2007.[14] The Army Chief Information Officer (CIO) G-6 instead decided that Microsoft SMS would provide configuration and software update capabilities for Army information systems. SMS was combined with Microsoft Operations Manager (MOM) to create a program known as Systems Management (SysMan). MOM brought operations, availability monitoring, remote access, service management, situational awareness and

[13] Andress, "Windows Patch Management Tools," 36–37.

[14] NETCOM, "NetOps Implementation Update: SCCVI Employment (eEye Retina / Remote Enterprise Manager)," *U.S. Army Network Enterprise Technology Command*, 2008, www.afcea.org/events/pastevents/documents/SCCVIUpdateBrief.ppt, 19.

event management to SysMan, and was always intended as a compliment to SMS.[15] Unfortunately, SMS did not address third-party patching concerns natively. Third-party patches could be deployed using SMS by taking advantage of its primitive software deployment capability, but did not use any detection logic. In essence, SMS simplify executed a script that installed an update onto a list of computers that had been identified as vulnerable in a separate network scan. This method required system administrators to create custom patches manually for each third-party vulnerability, then use an external scanner to identify vulnerable machines, and finally use SMS push update packages to specified clients. The same process could be accomplished without SMS by using a Visual Basic (VB) script or batch file.

In addition, SMS was supposed to be deployed Army-wide by September 30, 2008; as of February 2012, however, the deployment of SMS (renamed by Microsoft to SCCM in 2007) to all major Army units was still incomplete.[16,17] As a result, many Army Theater Network Operations and Security Centers (TNOSC) or regional Network Operations and Security Centers (NOSC) locally purchased their own solutions to meet their third-party patching needs. TNOSCs or NOSCs used Citadel Hercules, or turned to the expertise of computer programmers in their units to create custom scripts to deploy third-party updates. Overall, the Army was left with a comprehensive solution to deploy Microsoft updates, but a disjointed solution for dealing with third-party patches. As stated earlier, Army leadership in the CIO/G-6 recognized and acted on this problem prior to 2007 by selecting SMS as the Army enterprise solution for inventory and Configuration Management (CM), software distribution and patch remediation.[18] The selection of SMS by the Army was influenced by an annual analysis done by the Gartner group called the "Magic Quadrant for PC Configuration and Lifecycle Management," which compared

---

[15] Tim Ash and Mike Spragg, "NetOps Implementation Update (CMDB, SMS/MOM, SCTS.)," *U.S. Army Network Enterprise Technology Command*, August 22, 2007, www.afcea.org/events/pastevents/documents/Track4Session5-NetOpsUpdate.ppt, 12.

[16] Ibid., 19.

[17] Personal correspondence with U.S. Army Network Enterprise Technology Command official on February 3, 2012.

[18] Ash and Spragg, "NetOps Implementation Update (CMDB, SMS/MOM, SCTS.)," 12.

several enterprise CM tools, including Computer Associates (CA) Unicenter, IBM Tivoli, Altiris, Microsoft SMS and several others.[19] Gartner found that Microsoft SCCM cost significantly less than the comparable offerings from CA and IBM.[20] Of course, Gartner is just one of many analyst firms, but the recommendations of Gartner are highly valued by the U.S. Army. Prior to the decision to select Microsoft SMS, the Army had also entered into an Enterprise Licensing Agreement (ELA) with Microsoft. The ELA, which was signed in 2003, provided long-term, favorable pricing/licensing for SMS and other Microsoft products.[21] It is likely that the recommendations of Gartner, along with favorable pricing under the ELA, helped to steer decision makers into choosing SMS/SCCM over its competitors. Technology and the patching tools available to meet the Army's CM and third-party patching requirements have changed significantly since the Army made the decision to select SMS/SCCM.

A. PROBLEM STATEMENT

The U.S. Army is currently fielding Microsoft System Center Configuration Manager 2007 to provide a unified and comprehensive asset management system with the capability to mitigate vulnerabilities found in third-party applications on its information systems. However, it is unclear whether SCCM is the optimal choice for addressing this problem.

B. PURPOSE STATEMENT

The purpose of this thesis is to explore possible options that the Army may have to resolve third-party application vulnerabilities on its information systems. This study is concerned with determining whether a more effective and efficient way of mitigating third-party application vulnerabilities found on Army information systems exists in comparison to vulnerability mitigation systems currently in use, such as SCCM 2007.

---

[19] Ronni J. Colville and Michael A. Silver, *Magic Quadrant for PC Life Cycle Configuration Management 2005* (Gartner RAS Core Research Note G00131185), 2005.

[20] Personal correspondence with U.S. Army Network Enterprise Technology Command official on February 3, 2012.

[21] Mark Barnette and Adelia Wardle, "Microsoft Enterprise License Agreement," *Program Executive Office Enterprise Information Systems,* February 11, 2004.

C. RESEARCH QUESTIONS

- Q1. What would be an ideal solution to mitigate vulnerabilities in third-party applications on U.S. Army information systems?
    - SQ1: What would an ideal third-party patching solution look like from a system engineering perspective?
    - SQ2: Of existing third-party patching solutions, which comes the closest to meeting the ideal system as identified in the systems engineering analysis?

D. METHODS OF ANALYSIS

This thesis takes a system engineering approach to determine a notional ideal vulnerability management solution and then compare existing technologies to the notional ideal solution. Additionally, this thesis makes use of a cost benefit analysis to compare a select group of vulnerability management solutions to the notional ideal vulnerability management solution identified using the systems engineering approach.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. OVERVIEW

The lack of automated patching for both operating systems and third-party applications presents a very serious security risk. Research conducted by Gkantsidis, Karagiannis, Rodriguez, and Vojnović showed that over 95% of computers that did not receive automated Microsoft updates, required updates when the system user manually initiated an update request with an update server. In contrast, less than 10% of computers with automatic updates enabled required additional updates upon checking in with their update server.[22] This research was supported by Duebendorfer and Frei who found that 97% of web browsers with automatic updating enabled were running the latest version. In comparison, only 24% of web browsers that required the user to initiate the update process manually were running the latest version.[23] Keeping a computer system updated against all known vulnerabilities is extremely challenging but important to network security. An often cited 2004 study by CERT at Carnegie Mellon University found that, "about 95% of all network intrusions could be avoided by keeping systems up to date with appropriate patches."[24] Another study by Shostack found that the best way to reduce network security vulnerabilities was to close vulnerabilities than could be exploited with little skill. Closing those security vulnerabilities is best done by applying vendor supplied security patches. Shostack also noted that the majority of network break-ins take advantage of well-known security vulnerabilities where patches are available but have not been applied.[25] Once a network or information system is compromised, the cost to

---

[22] Christos Gkantsidis, Thomas Karagiannis, Pablo Rodriguez, and Milan Vojnović, "Planet Scale Software Updates," Proceedings of SIGCOMM, ACM, *SIGCOMM*, September 11–15, 2006, http://www.cs.ucr.edu/~tkarag/papers/planet_scale_updates.pdf.

[23] Thomas Duebendorfer and Steven Frei, *Why Silent Updates Boost Security*, Technical Report 302, TIK, ETH Zurich, 2009, http://www.techzoom.net/silent-updates.

[24] U.S. Government Accountability Office, *Agencies Face Challenges in Implementing Effective Software Patch Management Processes*, by Robert F. Dacey, (GAO-04-816T), Washington, DC: GPO, 2004, http://www.gao.gov/new.items/d04816t.pdf, 6.

[25] Adam Shostack, "Quantifying Patch Management," *Secure Business Quarterly*, 2003, http://www.homeport.org/~adam/sbq_patch_ashostack.pdf.

the organization in terms of monetary loss, and more importantly, intellectual property rights, is often costly and embarrassing.

B. THE COST OF CYBER ATTACKS

Monetary losses as a result of vulnerability exploits can be extremely high. A 2004 Congressional Research Study estimated that virus attacks cost $12.5 billion annually.[26] The 2009 Computer Crime and Security Survey reported that the average loss to a major U.S. business/institution per security incident to be $234,244, which represents a very significant decrease from the 2001 peak of $3.14 million per incident.[27] A 2005 survey done by the FBI indicated that annual losses due to computer crime for U.S. organizations to be at $67.2 billion.[28] Loss of national secrets can be even more damaging and difficult to quantify. A 2005 Time article by Elaine Shannon detailed how volumes of information were exfiltrated from DoD networks, as well as the world bank, by alleged Chinese hackers.[29] The newly published *Department of Defense Strategy for Operating in Cyberspace* stressed the nation's, and DoD's challenges in securing 15,000 networks and seven million information systems. The strategy noted that "every year, an amount of intellectual property larger than that contained in the library of congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies."[30]

A 2012 article in the *Wall Street Journal* reported that the Chinese government has a domestic policy of espionage in cyberspace. This fact has been acknowledged by the DoD, which sees the Chinese as "the world's most active and persistent practitioners

---

[26] Czumak III, "Recommendations for a Standardized Program Management Office (PMO) Time Compliance Network Order (TCNO) Patching Process," 1.

[27] Robert Richardson, "2009 Computer Crime and Security Survey," *Computer Security Institute*, 2009, http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf, 2–10.

[28] U.S. Government Accountability Office, *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, by Dave Powner, (GAO-07-705), Washington, DC: GPO, 2007, http://www.gao.gov/assets/270/262608.pdf, 2.

[29] Shannon Elaine, "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," *Time*, August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html.

[30] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, http://www.defense.gov/news/d20110714cyber.pdf, 1–4.

of cyber espionage today."[31] The article cites a recently declassified report to Congress in November 2011 from the office of the national counterintelligence executive that stated it was difficult to estimate the economic cost to the United States from stolen intellectual property or national secrets. The report considers the impact as "large," with significant effects on jobs, innovation and national security. The definition of "large" is assumed to be a loss of billions of dollars and millions of jobs.[32] A recent victim of one such cyber espionage attack, Lockheed Martin, provides an example of hackers targeting one of the United States' major defense contractors that supports the DoD. The latest attack used the Sykipot backdoor Trojan horse, and exploited vulnerabilities within Adobe Reader. A report by MSNBC found that the Sykipot Trojan horse was recently used by Chinese hackers to "hijack" the smartcards of U.S. government employees and access privileged information. Researchers from Alien Vault reported that the attacks spread via spear-phishing, which made use of targeted e-mails intended to trick victims into opening an infected PDF file, which then exploited security vulnerabilities in Adobe Reader.[33] As time passes, the number of cyber attacks that allow the penetration of Army/DoD networks and information systems can be expected to increase in frequency and sophistication.

The United States Department of Homeland Security (USDHS) recently published an extensive list of significant cyber incidents since 2006.[34] Of the 87 significant cyber incidents, 43 were reported from foreign governments or foreign corporations. The remaining 44 incidents occurred against various U.S. government agencies and major U.S. corporations. Furthermore, these incidents all occurred after the hackers gained access to networks through various third-party vulnerabilities and or other network vulnerabilities, such as phishing attacks. USDHS defined significant cyber crime

---

[31] Michael Chertoff, Mike McConnel, and William Lynn, "China's Cyber Thievery is National Policy- and Must Be Challenged," *Wall Street Journal*, January 27, 2012, http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html.

[32] Ibid.

[33] Matt Liebowitz, "Chinese Sykipot Malware Targets US Government," *MSNBC*, January 13, 2012, http://www.msnbc.msn.com/id/45985897/ns/technology_and_science-security/t/chinese-sykipot-malware-targets-us-government/#.TzBSiaX2aHw.

[34] U.S. Department of Homeland Security, "Significant Cyber Incidents Since 2006," January 19, 2012, https://www.hsdl.org/?view&did=12410.

as successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than one million dollars.

In 2009, USDHS planned to put the following measures in place to prevent future attacks and intrusion attempts by hackers:[35] Hiring additional personnel for the U.S. Computer Emergency Readiness Team (US-CERT) to bolster its around-the-clock identification and response to cyber threats and vulnerabilities. Expanding the EINSTEIN program[36] to all federal departments and agencies would help provide government officials much-needed early warning systems to identify unusual network traffic or pattern trends, and would signal a potential network threat. Consolidating and reducing the number of external Internet connections of the federal government internet infrastructure to improve efficiency and security to all federal ".gov" domains by creating a National Cyber Security Center to address cyber threats and improve cyber security mitigation efforts. Expanding the National Cyber Investigative Joint Task Force (NCIJTF) will now include the Secret Service and several other federal agencies not currently members. This task force will serve as a multi-agency national focal point for coordination, integration and sharing of pertinent information relating to cyber threats. DHS will further facilitate coordination and information sharing between the federal government and the private sector to reduce cyber risk and disseminate possible threat information and share best practices as outlined within the National Infrastructure Protection Plan (NIPP) framework. The final measure was to increase funding for IT security through the President's FY2009 budget request of $7.2 billion, which reflects an increase of $600 million over the FY2008 budget across the federal government for IT security.

Anyone who has been in the U.S. Army for longer than 10 years can remember a time when electricity was down at their workplace for an hour or longer. During this time, everyone starts to come out of their offices to investigate and congregate in common areas. Some staff is on the phone trying to ascertain the reason for the power

[35] U.S. Department of Homeland Security, "Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks," April 8, 2008, https://www.hsdl.org/?view&did=486707.

[36] The EINSTIEN software program was developed by US-CERT to monitor the network gateways of U.S. government agencies from unauthorized traffic.

outage, but it was generally realized that employees have an unprecedented reliance on IT systems. Luckily, power outages are extremely rare in this day and age on major U.S. Army posts. Similar to a power outage, network outages are also rare, but do happen. However, some work is still able to be done locally, even on an isolated IT system until services are restored, unlike a power outage where no work can be completed.

Network outages can be caused by a number of different factors to include power outages, network equipment faults, denial of service attacks and other software virus attacks to name but a few possibilities. The main outage focused upon involves third-party applications vulnerabilities exploited by phishing expeditions. It comes as no surprise to a system administrator that the major vulnerability within most networks is the end user, which phishing takes advantage of to exploit vulnerabilities in third-party applications. Timely updates of third-party applications are essential in a large network, but pose a significant challenge.

A survey of more than 400 data center and IT operations professionals commissioned by Emerson Network Power and conducted by Ponemon Institute in September 2010, reported that misconceptions about the impact of downtime and the frequency of those interruptions have become commonplace across the United States.[37] The survey brought to light the widening gap in perceptions between upper management and the "rank-and-file" IT staff. Even though upper management realized the economic importance of their company data services, they were not as "in-tune" with the everyday data center operations as the "rank-and-file" employees who were actually maintaining the IT infrastructure. This lack of perception could either be a disconnect on the part of the upper management, which is unfamiliar with the realities of operations at the ground level, or that the "rank-and-file" employees were lax in reporting actual network down time. The U.S. Army, unlike private companies, will not experience a decrease in revenue stream as a result of a network downtime; however, network downtime does make it more difficult to measure personnel efficiency.

[37] Emerson Network Power, "Understanding the Cost of Data Center Downtime: An Analysis of the Financial Impact on Infrastructure Vulnerability," 2011, http://emersonnetworkpower.com/en-US/Brands/Liebert/Documents/White%20Papers/data-center-uptime_24661-R05-11.pdf.

Even though the U.S. Army is not a private corporation, and as such not looking to increase its profits, it does, however, endeavor to be a good steward of taxpayer dollars. With ever shrinking defense budgets looming in the future, increased belt tightening and improving efficiency will continue to be as important today and in the future as it was in the past.

A well-known quote from Benjamin Franklin once said that, "an ounce of prevention equals a pound of cure." Patch and vulnerability management is the "ounce of prevention" compared to the "pound of cure" that is incident response.

To maintain the operational availability, confidentiality, and integrity of U.S. Army information technology IT systems, easy fiscal choices must be made.[38] The U.S. Army can choose not to be proactive and thus ignore third-party software vulnerabilities. This course of action (COA) will undoubtedly be the most expensive, as the cost to fix thousands or perhaps tens of thousands of computers would be in the millions of dollars. Another COA could be to monitor for patches manually and generate third-party software updates as the vulnerability presents itself. This COA is more cost effective than the first COA, but another COA is even more cost effective than the previous two. The third COA involves utilizing a commercial solution to check automatically for required new patches and deploy them. This solution would involve paying for the enterprise licenses for up to "744,000 U.S. Army Desktop computers"[39] and licensing costs for the individual software loaded on patching servers located at each U.S. Army NOSC, or TNOSC, to include continued contract, technical, updates and customer support for five years.

When considering the costs involved in maintaining U.S. Army information systems, initial costs, maintenance and operation costs and life-cycle costs of the system to be purchased must be quantified. Along those lines, it must also be possible to measure

---

[38] Peter Mell, Tiffany Bergeron, and David Henning, *Creating a Patch and Vulnerability Management Program: Recommendations of the National Institute of Standards and Technology (NIST)*, (Special Publication 800–40, Gaithersburg, MD, 2005), http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

[39] Gary Sheftick and Delawese Fulton, "Army Migrating to Vista," *Army News Service*, May 20, 2009, http://www.army.mil/article/21389/army-migrating-computers-to-vista/.

a proposed purchase with a well-known industry standard or standards. The next section explores the DoD concept of Cost-Benefit Analysis (CBA).

1. What Is a Cost-Benefit Analysis?

CBA is a technique used to evaluate a project or investment by comparing the economic costs with the economic benefits of the activity. CBA has several objectives. First, CBA can be used to evaluate the economic merit of a project. Second, the results from a series of CBAs can be used to compare competing projects. CBA can be used to assess business decisions, to examine the worth of public investments, or to assess the wisdom of using natural resources or altering environmental conditions. Ultimately, CBA aims to examine potential actions with the objective of increasing Return on Investment (ROI). Regardless of the aim, all cost-benefit analyses have several properties in common. A CBA begins with a problem to be solved. For example, a community may have the goal of alleviating congestion on roads in an area. Various projects that might solve the particular problem are then identified. As an example, alternative projects to alleviate road congestion in an area might include a new highway, a public bus system, or a light rail system. The costs and benefits of these various projects would be identified, calculated, and compared. Decisions are typically not made solely on the basis of CBA, but CBA is useful and sometimes required by law. Without a doubt, results from a CBA can be used to raise the level of financial awareness surrounding a project but perhaps more importantly, it helps leaders make informed decisions. Some think of CBA as a narrow financial tool. However, this belief underestimates its versatility in addressing intangible values. Recent methodologies can help estimate the value to decision makers of intangible benefits. At the very least, CBA can be used as the basis of comparison between alternative ways of achieving an intangible benefit, such as different forms of treatment in health care.

2. Where Cost-Effectiveness Analysis Fits into Decision Making

Cost-Effectiveness Analysis (CEA) was developed specifically as part of efforts to extend economic criteria to assess military spending alternatives. In the 1960s, the RAND Corporation devised rules for allocating resources to achieve military objectives

to assign a perceived valuation for measurement.[40] CEA is a form of economic analysis that compares the relative costs and outcomes (effects) of two or more courses of action. CEA is distinct from CBA, which assigns a monetary value to the measure of effect. CEA often used in the field of health services, where it may be inappropriate to monetize health effect. CEA enables application of rational economic logic to assess policies for which it is extremely difficult if not impossible to value benefits in monetary terms. "The first systematic attempt to apply cost-benefit analysis to government economic decisions probably started in the United States. Here it was a matter of practical engineering, with the attempt, starting about 1900, to improve harbor and river navigation. Here it was "in origin an administrative device owing nothing to economic theory."[41] It was not until 1965, after a CBA was first utilized in justifying that year's projected DoD budget, that an impressed President Johnson directed that the Planning, Programming, and Budgeting System (PPBS) activity be further utilized throughout the federal government. Even though the military does not derive any increase in revenue or a decrease in measured expenditures as a result for certain policy choices, the CBA is a natural choice to utilize in this instance as the authors attempt to monetize the benefits of utilizing one of the many automatic third-party application remediation products available on the market today.

3. What is the True Cost of a Computer Virus?

Depending on whose estimate is relied upon, the worldwide cost of the *LoveLetter* worm is placed somewhere between tens of millions to possibly one billion dollars in damage. Whichever is correct, the estimates are staggering. Just how are such costs calculated? Can they be substantiated? What costs might be incurred? Hard costs, such as technician costs to mitigate the infection, costs to replace any hardware or even costs to upgrade hardware in hopes of mitigating a future similar virus are relatively simple to calculate. Typically, "soft-costs" calculations are much harder to quantify, which

[40] H. G. Massey, David Novick, and R. E. Peterson, *Cost Measurement: Tools and Methodology for Cost Effectiveness Analysis* (Santa Monica, CA: The RAND Corporation, February 1972).

[41] E. S. Quade, *A History of Cost-Effectiveness* (Santa Monica, CA: The RAND Corporation April, 1971).

includes intangibles, such as loss of opportunity combined with the more realistic loss of productivity, or more importantly and easier to measure, lost person hours.

4. Loss of Opportunity

Hypothetical Company *A* makes widgets that it badly wants to sell to Company *B*. Deals are on the table, ready to be signed. Unfortunately for Company *A*, a competitor, Company *C*, also wants to sell to Company *B*. The most important factor to Company *B* is whether its widgets will be delivered on time; thus the reliability of the competing companies will be the deciding factor. Company *A* has promised to e-mail its final proposal by Monday at 4 p.m. At 2 p.m., a virus infiltrates its organization and all the mail servers are shut down shortly thereafter. As luck would have it, Company *A*'s proposal is stuck in the queue and never leaves the company servers. As 4 p.m. comes and goes, Company *B* has only received one proposal —from Company *C*. Guess to whom the deal is awarded? This situation is a worst case scenario, but it illustrates the importance of virus mitigation.

5. Loss of Productivity

A public relations firm, PR One, is heavily involved with technology publications and various industry analysts. It constantly corresponds via e-mail, sets tour schedules, sends press releases, and maintains its valuable contacts. Struck by an e-mail worm, PR One is not able to function for several hours as its mail servers have all been shut down. Telephoning contacts is not an option, as everyone in its industry is focused solely on this latest virus attack. Although no known opportunities were lost, several PR personnel were still sitting around, waiting. In other words, they were not productive during this time while the servers were down.

6. Lost Person-Hours

Not quite the same as loss of productivity, but lost person hours usually only affect IT personnel. Their workloads have tripled, and are busy due to a virus outbreak; the fact is that the work they should have been doing, such as finalizing the E-Commerce backbone, is not getting done. Every hour they spend working on the latest malicious

code emergency means pushing off the projects on which they should be working. Even with overtime, these hours cannot simply be recaptured. Thus, everyone's schedule is adversely affected. In addition, an actual cost is associated with the virus if an IT employee is being paid for overtime to mitigate the infection. Technically, the same could be said for a regular employee when prevented from completing tasks on time and forced to work overtime to complete assigned tasks or job to meet a deadline. The bottom line, however, is the fact that it is not possible to regain those lost hours.

7. Life-Cycle Costing

In the early 1960s, the DoD realized that its initial acquisition costs were traditionally small when compared to the cost of the system over that system's entire lifetime. Thus, it reengineered its business model and made it mandatory for acquisition offices to start looking at the projected costs of the system over its lifetime in addition to its price bid. This new system was coined "Life-Cycle Cost Methodology." This method of costing is used in the analysis as required by the federal government regulations.

Symbolically, LCC appears as the following.

$$\text{Life-Cycle Costing} = \sum_{k=(m-1)}^{n} \frac{C_k}{(1+i)^k}$$

where m is the number of years in the development/acquisition phase, n is the operational lifetime, i is the interest (discount) rate, and C_k is the cost incurred in the kth year. This equation basically provides the Net Present Value (NPV) at the end of period discounting.[42]

To utilize the formula, the following must be executed.

- Estimate the useful life of the system
- Estimate the yearly costs over the life-cycle
- Choose a discount rate (Use OMB Circular A-94, Appendix C)

[42] I. Eisenberger and G. Lorden, *Life-Cycle Costing: Practical Considerations*, DSN Progress Report 42–40, May and June 1977.

The purpose of the OMB Circular A-94 is to set forth clear guidance from the federal government for future potential considerations of projects paid for by U.S. taxpayer dollars. It also provides general guidance for conducting benefit-cost and cost-effectiveness analysis. It also puts forth guidance on the proper use of the discount rates to be utilized when evaluating any federal program whose benefits and costs are considered over a period of time. Appendix C, within Circular No. A-94, also sets forth the historic discount rates in both nominal rates that represent the dollars that must be paid to settle a debt and includes inflation, and real rates that represent the constant purchasing power over time, from 1979 to 2012.[43] For the purpose of this study, nominal dollars and the discount rate from 2009 are used for all CBA calculations.

C. TRENDS IN CYBER ATTACKS

Statistics from the National Vulnerability Database (NVD) show a disturbing trend in the number of software flaws recorded annually. The NVD first began recording software flaws in 1988, during which time, two vulnerabilities were reported. By 1997, only 211 software vulnerabilities were reported for the year, which represents modest growth considering the time frame. In contrast, the number of vulnerabilities rose from 1,020 in 2000 to a peak of 6,608 in 2006, a six-fold increase. This time period coincided with the explosion of the Internet and e-commerce. Since 2006, the number of vulnerabilities reported annually has seen a steady decline. The last full year on record, 2011, recorded 4,151 vulnerabilities (Figure 2),[44] which represents an average of slightly over 11 patches released per day over the entire year.

[43] Office of Management and Budget, *Guidelines and Discount Rate for Benefit-Cost Analysis of Federal Programs*, Circular No.A-94, April 19, 1992.

[44] National Vulnerability Database, "NVD's CVE and CCE Statistics Query Page," 2011, http://nvd.nist.gov/statistics.cfm.

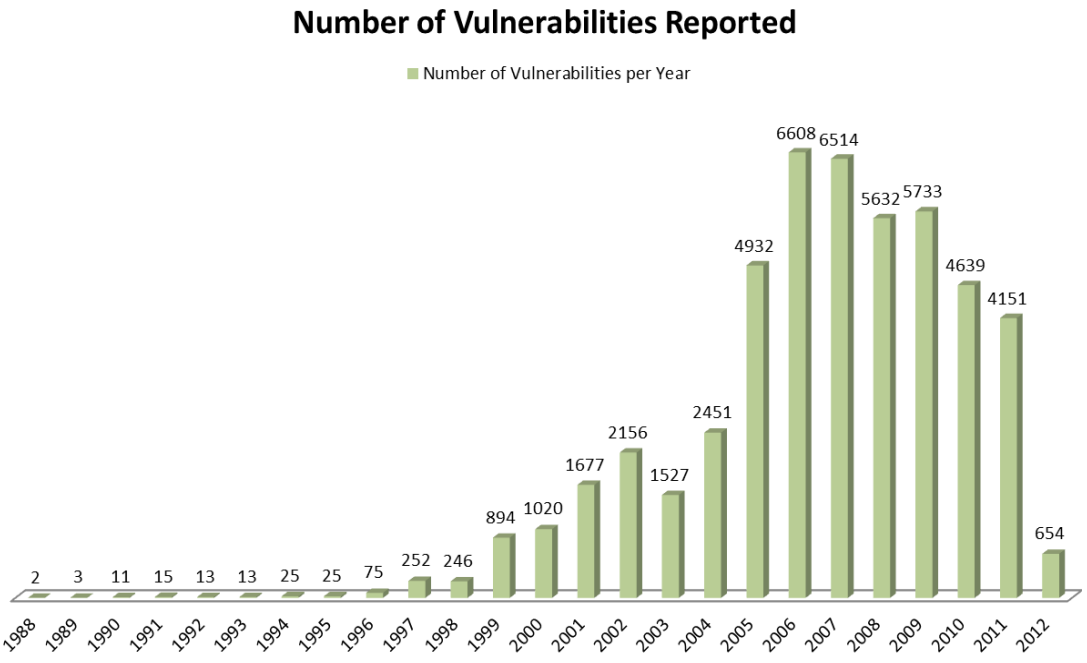


Figure 2. Software Flaws Reported Annually[45]

Another disturbing trend is the diminishing time between a software vulnerability being announced to an exploit being created to take advantage of the vulnerability. Pfleeger and Lawrence reported in their book, *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*, that in 2009, Microsoft released patches for Internet Explorer and within two days, exploits were live and targeting unpatched systems,[46] which indicates that cyber criminals have become very skilled at reverse engineering patches to develop exploits. Even more troubling is the fact that some software vendors are very lax about releasing patches for known vulnerabilities. Oracle is reported to have released no patches from January 2005 to March 2006, which allowed reported vulnerabilities to go unattended for over a year.[47] Other corporations, such as Microsoft, have a history of releasing patches very quickly when vulnerabilities are discovered.

---

[45] National Vulnerability Database, "NVD's CVE and CCE Statistics Query Page."

[46] Charles P. Pfleeger and Shari L. Pfleeger, *Analyzing Computer Security: A Threat/ Vulnerability / Countermeasure Approach* (Prentice Hall, New Jersey, 2011), 137.

[47] Ibid.

Yet another trend even more difficult to deal with is the increased use of zero day exploits in cyber attacks. A zero day exploit takes advantage of a software vulnerability that has been discovered, but does not yet have patch ready for release to address the software vulnerability.[48] For this reason, software vendors will not normally disclose to the public that their software has a vulnerability until they have a patch for it. Thus, hackers are not tipped off that a vulnerability exists before a patch is ready. Professional or state sponsored hackers actively work to find undiscovered software exploits, and keep them secret until they are ready to launch a true zero day attack. State sponsor hackers are much more likely pursue zero day exploits because they have the expertise and resources to discover a software vulnerability and develop an exploit. The zero day exploit provides the state-sponsored hacker with the capability to gain access to an adversary's information system(s) almost at will, at least for the first time it is used.

Once a zero day exploit is discovered, but no patch is available, the best course of action is to avoid using the software that contains the vulnerability. After the discovery of a zero day exploit, software developers will develop a patch that closes the vulnerability in the affected software. Once the patch is released, zero day exploit becomes a regular exploit that makes its way into the automated toolkits used by script kiddies. In December 2011, Lockheed Martin and Defense Security Information Exchange reported a zero day exploit, which they were also victims of, to Adobe. The exploit took advantage of vulnerabilities in Adobe PDF Reader and Acrobat. Unfortunately, hackers were able to do an undisclosed amount of damage to several defense contractors until Adobe released patches for its products.[49]

A four-year study done by Verizon Business Investigative Response team of over 500 incidents found that most data breaches often go undiscovered for long periods of time, and are usually discovered by an outside organization and not the victim. Researchers also found that cyber criminals have continued to chase the easy money.

---

[48] SANS, "Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines," August 10, 2009, http://www.sans.org/critical-security-controls.

[49] Fahmida Y. Rashid, "Adobe Zero-Day Exploit Targeted Defense Contractors," December 7, 2011, *eWEEK*, http://www.eweek.com/c/a/Security/Adobe-ZeroDay-Exploit-Targeted-Defense-Contractors-383203/.

They continue to achieve the most success against businesses that fail to employ robust network security practices, including the retail and food service industries as shown in Figure 3. In contrast, data breaches against government agencies comprised only 2% of the 500 incidents due to the relative difficulty of achieving success.[50]

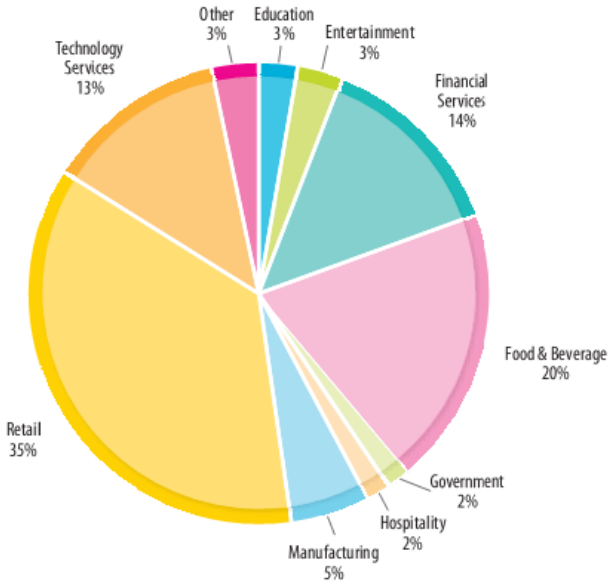


Figure 3. Data Breaches Between 2004–2007[51]

Of the data breaches investigated, 73% came from external threats, such as hackers, organized crime, or even foreign governments as shown in Figure 4. Eighteen percent of the data breaches involved disgruntled employees and employees who unintentionally compromised data. In the remaining 9% of data breaches, the source could not be conclusively determined. Partners accounted for 39% of the internal data breaches; who are competitors looking to steal trade secrets or gain the upper hand on their completion. More than 25% of the data breaches involved a combination of internal

[50] Wade H. Baker, David C. Hylender, and Andrew J. Valentine, "2008 Data Breach Investigations Report," *Verizon Business Risk Team*, 2008, http://www.verizonbusiness.com/resources/security/databreachreport.pdf, 8.

[51] Ibid.

and external sources,[52] which could be a system administrator inside an organization passing network credentials to an outside entity or in a scenario investigators saw frequently, an employee of the organization had network credentials compromised that allowed outsiders privileged access to the organization.

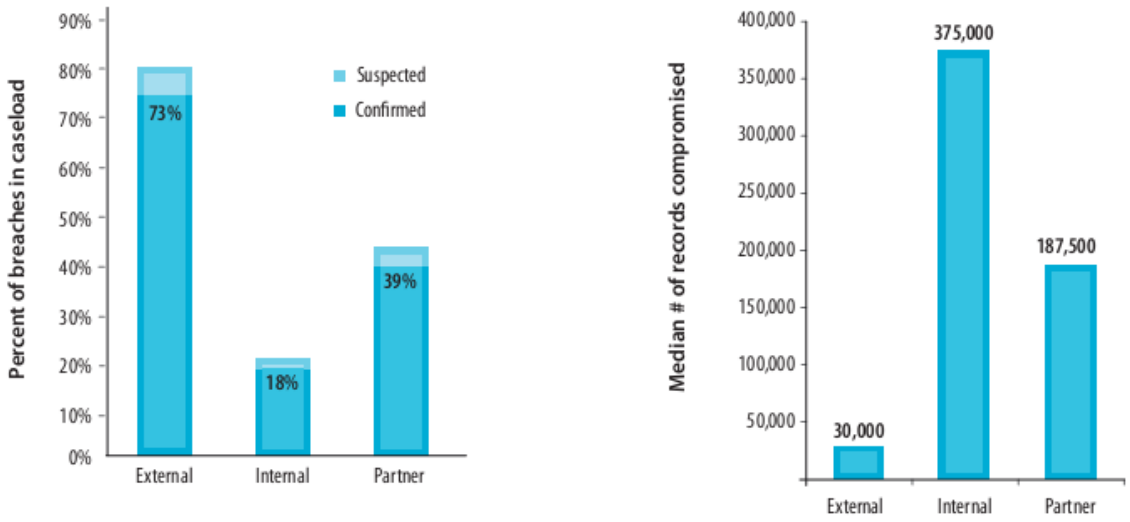


Figure 4. Data Breaches Between and Records Compromised Between 2004–2007[53]

Despite the fact that external threats comprise the majority of data breaches, internal threats are more damaging. Figure 4 shows that insiders exfiltrated 10-times more data on average than outsiders because of privileged access, their ability to remain undetected and the special knowledge they have over where the data they want to steal is stored.[54] Figure 5 shows the origin of the cyber attackers' IP addresses. Researchers noted that attacks originating from China and Vietnam tended to involve software application exploits that resulted in data theft. Attacks originating from the Middle East tended to result in the defacement of websites. Attacks coming from Eastern Europe and Russia were directed primarily at Point of Sale (PoS) systems.[55] The researchers found

[52] Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report," 10.

[53] Ibid.," 10–11.

[54] Ibid., 11.

[55] Ibid., 12.

that between 2004 and 2007, the number of attacks tied to organized crime doubled each year.

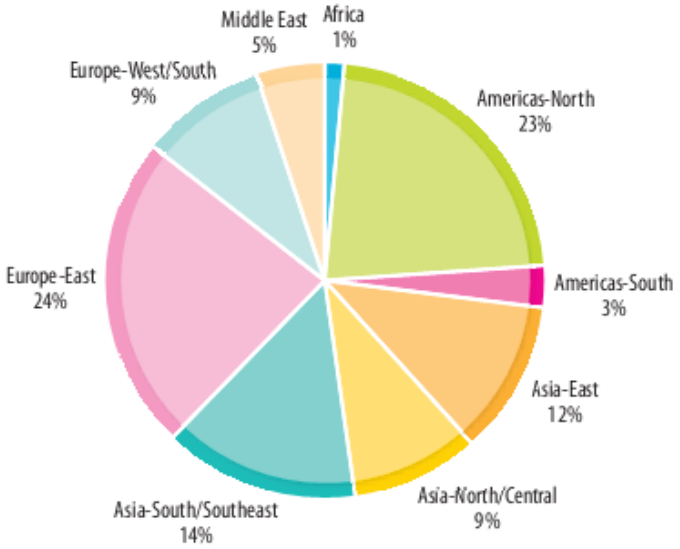


Figure 5. Origin of Attacking IP Addresses[56]

Investigators concluded that hacking comprised 59% of attacks, followed by malicious code, at 31%.[57] In nearly all of the recorded cases, error was a contributing factor. Error includes poor decisions, improper configuration, lack of compliance with company policy and oversight. Of the data breaches completed by hacking, 18% exploited a known vulnerability and 5% exploited zero-day vulnerabilities as shown in Figure 6. These numbers conflict with other sources that report that the vast majority of exploited vulnerabilities could have been prevented if available patches had been applied. It is possible that the graph was poorly worded and the authors meant to include the application/service layer and OS/platform layer into the "Exploits Known" group. Also of interest is the 15% statistic cited by the authors for "Use of Back Door." Back doors are usually installed by some form of malicious software, which either takes advantage of a known or unknown vulnerability. The fact that back doors were included separately

[56] Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report," 12.

[57] Ibid., 12–13.

supports the assertion that the data was most likely correct, but was labeled poorly in the graph.

Of the known exploits, all could have been prevented had vendor-supplied patches been applied within one month. Figure 7 illustrates how long a patch was available for a known vulnerability. A full 96% of known exploits were successful on information systems that had patches available for at least three months,[58] which suggests that organizations should emphasize completeness of patching over patching clients as quickly as possible.

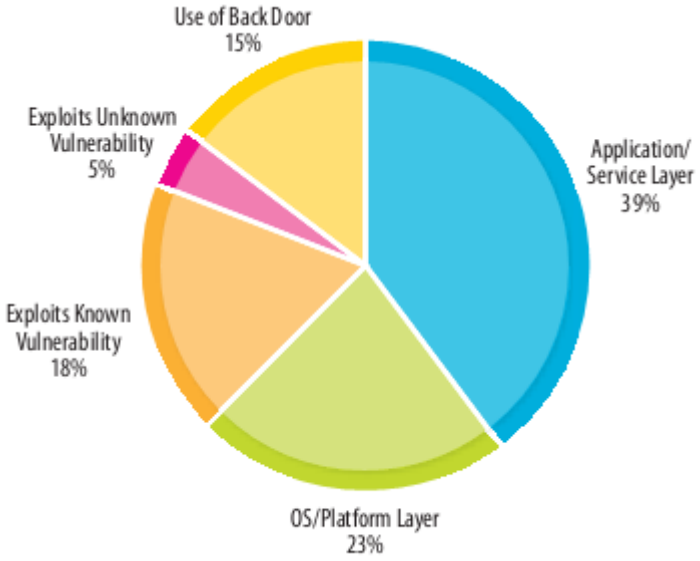


Figure 6. Attack Vectors by Hackers[59]

[58] Baker, Hylender, and Valentine,"2008 Data Breach Investigations Report," 15.

[59] Ibid.

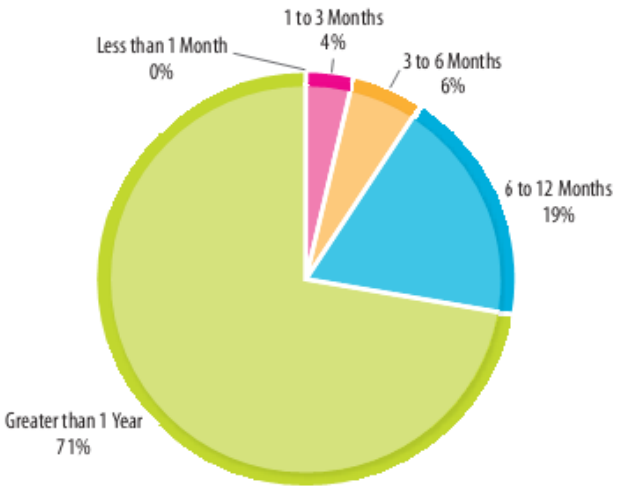


Figure 7. Patch Availability at the Time of Attack[60]

Investigators also looked at the amount of skill needed by cyber criminals to complete their attacks. Figure 8 shows the level of skill involved in completing a cyber attack. They found that the majority of attacks involved low skill, and were undertaken by script kiddies utilizing automated tools they downloaded from the Internet. Moderate skill on the part of the attacker accounted for 28% of attacks. This group includes cyber criminals with significant resources but limited programming skill. Cyber criminals with high skill comprised 17% of attacks. These attacks are primarily state or organized crime sponsored with extensive funding. Cyber criminals comprising the high skill group are most likely to use zero-day attacks, or other sophisticated techniques.

[60] Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report," 15.

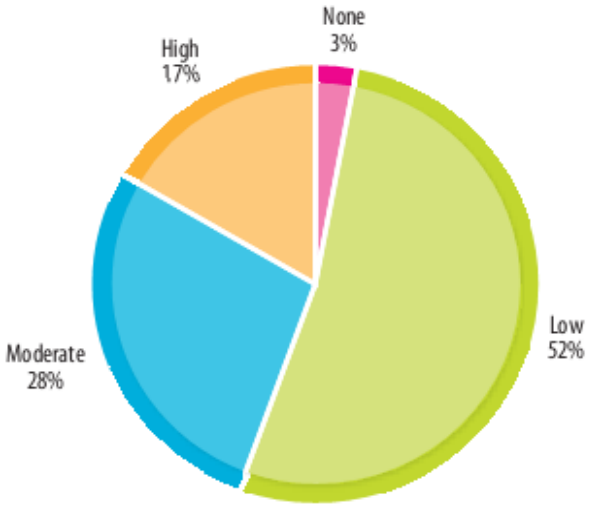


Figure 8. Attacker Skill Required[61]

Highly skilled and well-funded cyber criminals have the ability to breach nearly any network given enough time. In his article, "The Secret War," Adam Piore argued that "even with cooperation most security experts believe that keeping a capable and determined adversary out of a system is impossible."[62] It is the age old problem of defending. Defenders must expend resources to protect all of their assets, while the attacker is free to pick and choose a single point or targeted vulnerability to attack.

Researchers at Verizon make the point it is the defender's job to make the cost of breaching the defender's defense greater than the benefit gained by the attacker from breaching said defenses. The hope is that cyber criminals will pick a softer target to reach their objectives. However, sometimes the gain for the attackers is so lucrative that they are willing to expend considerable resources to breach the defenders' network.[63]

As mentioned earlier, most organizations take a long time to learn that they are the victims of a cyber attack. As illustrated in Figure 9, in 63% of the cases, it took at least one month to discover that an attack even took place. In contrast, it generally takes attackers a small amount of time to steal data successfully once they gain access to an

[61] Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report," 18.

[62] Adam Piore, "The Secret War," *Popular Mechanics*, January 2012, 52–57.

[63] Baker, Hylender and Valentine, "2008 Data Breach Investigations Report," 17–18.

information system. On 47% of cases, access was gained in less than 24 hours. Getting rid of an attacker once a network has been compromised was found to be a difficult and time consuming task, with most organizations taking weeks to months to re-secure their networks.[64] Researchers believe that length of time results because most organizations do not know how to respond properly to a real-world attack.

Figure 9. Time from Compromise to Discovery[65]

Most organizations discover they are victims of a cyber attack because of a report by an entity outside of their organization as shown in Figure 10. Researchers in the study also found that most organizations collect and store logs on their information systems and many conduct other forms of analytics, which should have allowed them to at least detect that an attack had occurred. In most organizations, these activities are done as a formality; the data gathered from log files or analytic tools is seldom utilized. In 82% of cases, researchers found that organizations had the capability to discover the data breach themselves, but only occurred in 7% of the incidents.[66]

[64] Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report," 22–23.

[65] Ibid., 22.

[66] Ibid., 23.

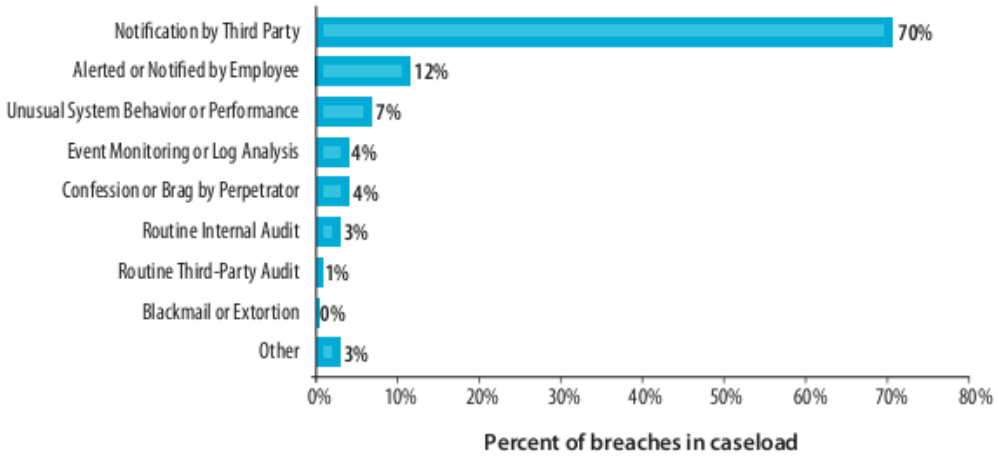


Figure 10. Detection Method for Cyber Attack[67]

The study concluded by stating that in 87% of data breaches investigated, data theft could have been avoided if reasonable security measures were in place at the time of the attack. The study emphasized the importance of strengthening the inner defenses of the network, and importantly, the individual workstation.[68]

Another trend in network attacks, which has been increasing over time, is the use of botnets. Botnets are logical groupings of computers, compromised by malware or a virus, which attackers can remotely control without the knowledge of the systems owner. Cyber criminals make use of command and control software to mount coordinated and fully automated attacks against the most robust networks. Botnets, such as *Conficker*, are believed to have contained in excess of 10 million computers.[69] Botnet attacks can take many forms, but they commonly distribute spam, viruses and conduct Denial of Service (DoS) attacks. Botnets are a particularly difficult problem because they are hidden and engineered so that most anti-virus programs cannot detect them. Standard security practices, such as the use of a corporate Demilitarized Zone (DMZ), strong host anti-

[67] Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report."

[68] Ibid., 26.

[69] CIO, "8 Elements of Complete Vulnerability Management," *Chief Information Officer Online*, October 2009, http://www.cio.com/documents/whitepapers/VulnerabilityManagement.pdf.

virus software, strong passwords and fully patched software are the best preventative actions to avoid infection.[70]

D. AUTOMATED PATCHING

Given the sheer volume of software updates released annually, combined with the growing number of applications on each individual workstation, the need for automated patching solutions was clear to most IT system administrators by the mid to late 1990s. Up until that point, it was still reasonable to update computers manually because of the relatively small number of patches being released, combined with a generally lower density of information systems in a typical business. A 2009 study by Gerace and Cavusoglu, looking at the critical elements of patch management, found that 83.5% of 114 respondents in the corporate, government, education and health care sector were using some form of automated patch installation,[71] which included either SUS, Windows update or a third-party patching solution, such as HF NetChk. It is surprising that a full 16.5% were still using manual patching, given the ease of using SUS or Windows update. The study did not distinguish between operating system and third-party updates. Gerace and Cavusglu also noted a perception among respondents that "senior executive support" was not very important to the patching process. This perception is not terribly surprising, as system administrators tend to look at the technical aspects of updating information systems, and often neglect the coordination and support tasks necessary to patch a large organization's information systems successfully. One way that executive support is needed is to authorize update periods during which patches can be installed without administrators having to worry about disrupting the productivity of the organization. Another need for executive support concerns funding. System administrators need an adequate level of monetary support to conduct lifecycle replacement on aging information systems, pay for service contracts and procure new software. The study

[70] Mindi McDowell, "Cyber Security Tip ST06-001: Understanding Hidden Threats: Rootkits and Botnets," *US-Cert*, August 26, 2011, http://www.us-cert.gov/cas/tips/ST06-001.html.

[71] Thomas Gerace and Huseyin Cavusoglu,"The Critical Elements of the Patch Management Process," *Communications of the ACM* 52, no. 8 (August 2009): 117–121, http://doi.acm.org/10.1145/1536616.1536646

concluded by noting that organizations that reported the use of automated patching were the most effective at applying updates.

Most organizations and their system administrators, including the U.S. Army, were quick to adopt a patching system that kept their Windows-based operating systems updated. Microsoft released SUS in 2003 to address the need to automate operating system updates. Block noted in a 2007 field report from Iraq that SUS was a good tool for deploying operating system patches, but it did not allow computers to be segregated into different groups based on their operating system or use. In Block's case, most of his machines were Standard Army Management Information Systems (STAMIS), which meant they were not on the same patching cycle as non-program managed computers. The release of WSUS in 2005, remedied this shortcoming, as well as added the ability to deploy additional software, including updates to virtually all Microsoft products, but most significantly, Microsoft Office. Block further noted that once the SUS was setup, the system administrator only needed to approve new patches. He contended that this made administering the SUS and keeping the operating systems of Microsoft-based computers patched a "simple" task.[72] However, industry concerns do exist about the security of the patching process itself.

A study by Bellissimo, Burgess and Fu found that automated patching systems can also be a point of weakness in the update process. The study found that certain patching solutions are vulnerable to man-in-the-middle attacks, although the study admitted that they did not specifically examine the WSUS system.[73] The study explained that Microsoft uses a system of RSA-SHA1 encrypted signatures and concluded that Microsoft and Apple have superior update systems in comparison to third-party automated updates because they have centralized control over the updating process, which allows them to control the distribution of updates using trusted public keys.[74] This

---

[72] Jerome P. Brock, "CSSAMO Experiences in Operation Iraqi Freedom," *Army Logistician*, 2007, http://www.almc.army.mil/alog/issues/JanFeb07/cssamo_exper.html.

[73] Anthony Bellissimo, John Burgess, and Kevin Fu, "Secure Software Updates: Disappointments and New Challenges," Proceedings of the 1st USENIX Workshop on Hot Topics in Security, *USENIX Association*, 2006, http://static.usenix.org/event/hotsec06/tech/full_papers/bellissimo/bellissimo.pdf, 37.

[74] Ibid., 40.

control supports a requirement for all third-party patching solutions to make use of a Private Key Infrastructure (PKI) system to prevent man-in-the-middle and replay attacks.

The adoption of WSUS by the U.S. Army, the DoD, as well as the majority of corporate America, demonstrated that nearly all established organizations recognized the need for an automated patching tool to secure their information systems. The decision by the U.S. Army to make Microsoft Windows the standard operating system for its desktop, as well as server environment, allowed WSUS to be extremely effective at mitigating Microsoft vulnerabilities. However, the rise in third-party application vulnerabilities limited the positive impact that WSUS had in patching information systems. WSUS deployments were very effective at deploying Microsoft patches, which quickly closed the exploitation period available to cyber criminals for attacks against Microsoft applications. Each third-party application relies on its own internal patching system, independent of WSUS, which generally requires user interaction to install. The implication is that third-party vulnerabilities are often left unpatched, or they are patched more slowly than Microsoft vulnerabilities. This impact is seen in statistics from the National Vulnerability Databases. In 2010, the NVD recorded that of the top 13 applications with the most reported vulnerabilities; only two were from Microsoft, as shown in Figure 11.[75] The applications with the most reported vulnerabilities are now web browsers, including Google Chrome, Apple Safari and Mozilla Firefox.[76] At least part of the reason for more vulnerabilities is that cyber criminals expend a great deal of effort in finding new vulnerabilities in free, widely used third-party applications because they represent an outstanding attack vector and offer a favorable ROI for the cyber criminal. The SANS Institute supported the data gathered by the NVD by stating that "un-patched client applications are the most important security risk facing organizations today."[77]

---

[75] National Vulnerability Database, "NVD's CVE and CCE Statistics Query Page," 2011, http://nvd.nist.gov/statistics.cfm.

[76] Bit 9, "Web Browsers, Desktop Software Top Dirty Dozen Apps List," 2010, http://www.bit9.com/company/news-release-details.php?id=175.

[77] SANS, "Top Cyber Security Risks—Executive Summary," September 2009, http://www.sans.org/top-cyber-security-risks/summary.php.

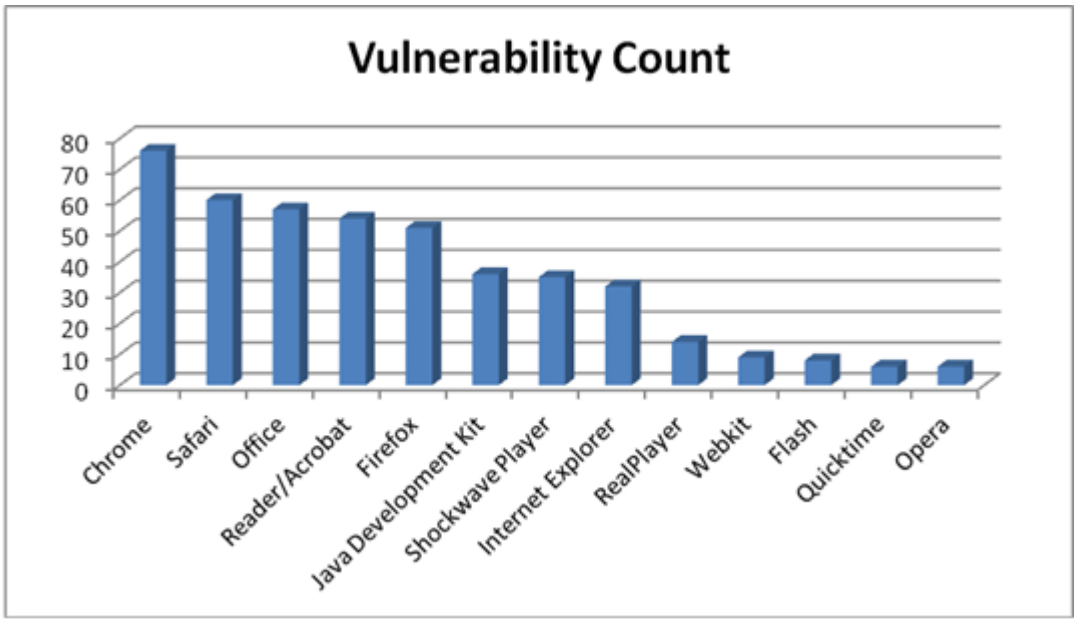


Figure 11. Most Frequently Targeted Applications of 2010[78]

The exploitation of client-side vulnerabilities is most commonly done by targeted e-mails; known as spear phishing, and also by enticing users to visit infected websites. Once a user opens an infected e-mail, or visits an infected website, malicious code is executed that exploits software vulnerabilities. As mentioned earlier, the vulnerabilities targeted have been in commonly used third-party applications, such as Adobe Reader, Apple QuickTime, Adobe Flash, or Sun Java, to name a few as Figure 12 illustrates. In 2009, SANS recorded Adobe PDF Reader was very widely attacked, as was Adobe Flash and Sun Java. A SANs report stated, "During the last few years, the number of vulnerabilities being discovered in applications is far greater than the number of vulnerabilities discovered in operating systems."[79]

[78] National Vulnerability Database, "NVD's CVE and CCE Statistics Query Page."

[79] SANS, "Top Cyber Security Risks—Executive Summary."

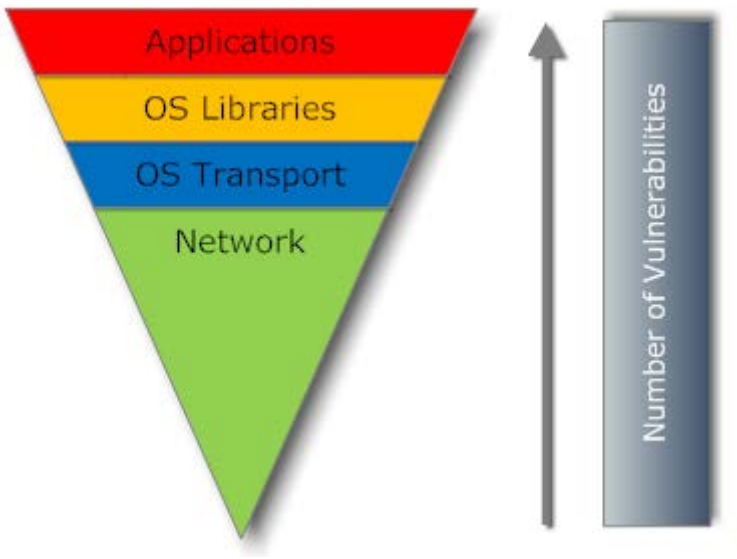


Figure 12. Number of Vulnerabilities in Network, OS and Applications[80]

Free third-party applications make such lucrative targets because they are installed on nearly all client workstations regardless of organization and are often patched slowly or not at all. Most popular third-party applications use automatic update mechanisms, which interrupt the user to ask their permission to install a security update. This method is used by Sun Java, Apple QuickTime/Safari/iTunes, Adobe Flash/Reader/Acrobat and many others. Not surprisingly, most users react to the annoyance of an update request by ignoring or cancelling it. Google made the correct choice with the update mechanism on its popular chrome browser, which automatically updates the browser to the latest version without user consent.

A 2011 study done by CSIS found that up to 85% of virus/malware infections of Windows computers occur due to the use of automated exploit kits by cyber criminals. The study looked at 13,210 Danish users and found that 31.3% of their personal and corporate PCs were infected with malware/viruses. All of the attacks in the study took advantage of a web browser as the attack vector. Figure 13 shows the six specific applications that comprised 99.8% of the exploits completed. These applications should seem familiar by now, but are still worth mentioning. Sun Java JRE, Adobe

[80] SANS, "Top Cyber Security Risks—Executive Summary."

Reader/Acrobat and Adobe Flash comprised 85% of the observed exploits, while Microsoft Internet Explorer, Windows HCP and Apple QuickTime the remaining 15%.[81] The study concluded by suggesting that nearly all successful attacks by cyber criminals using commercially available exploit kits could have been prevented by updating six specific applications. It is fairly obvious why these six applications are targeted as they are used on nearly every Windows computer on the Internet and nearly all have frequent vulnerabilities reported. This narrow attack vector for cyber criminals increases their chances of success.

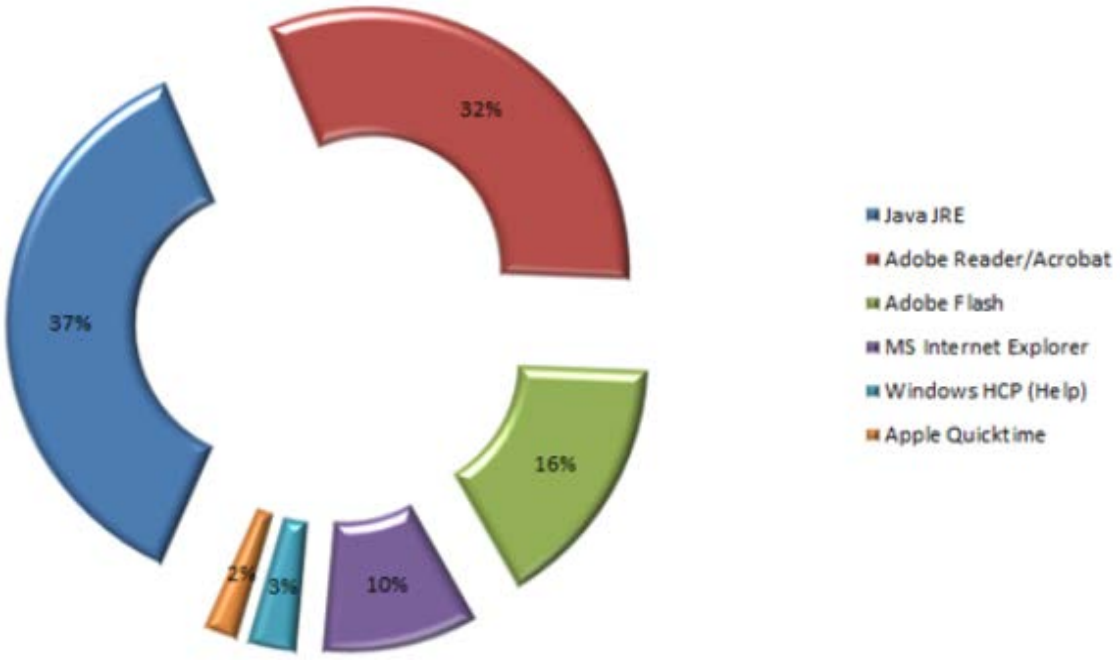


Figure 13. Applications Most Exploited by Malware/Viruses[82]

SANS also noted that major organizations take at least twice as long to remediate third-party vulnerabilities in comparison to patching operating system vulnerabilities.[83] The fact that Microsoft applications are no longer the favored exploitation vector is a

[81] Peter Kruse, "This is How Windows Gets Infected with Malware," *CSIS Security Group*, September 27, 2011, http://www.csis.dk/en/csis/news/3321/.

[82] Ibid.

[83] SANS, "Top Cyber Security Risks – Executive Summary."

clear indicator that hackers recognize the strength of the WSUS automated update system when faced with known exploits. Hackers did not take long to realize that their chances of success were improved significantly if they shifted their focus from operating system exploits to third-party application exploits. Safeguarding against third-party software exploits has proven to be a significant challenge for the U.S. Army, as well as the DoD.

A 2007 thesis by Lt. Michael Czumak at the Air Force Institute of Technology looked at resolving vulnerabilities in Air Force program managed information systems, which are very similar to Army STAMIS systems. Lt. Czumak found that automating the patching of information system saved system administrators a great deal of time and improved the probability of patching success. Automation of patching reduced the workload of network administrators and IA personnel, and allowed them to focus on information systems that automated patching could not remediate. Although Lt. Czumak did not state it explicitly in his thesis, a very high probability exists that manual updating had to be completed on third-party applications due to the lack of a deployed automated patching solution. Lt. Czumak also found that many organizations within the Air Force PM community wanted an automated patching system for third-party applications, but did not have one available.[84]

1. Army Vulnerability Management Experiences

The widespread adoption of a means to automate patching for third-party application vulnerabilities was slow to materialize in the Army as well. CPT Sabovich served as the Network Operations and Security chief for the U.S. Army in Hawaii, from 2007 to 2008, and inherited an extremely effective robust WSUS infrastructure at automating Microsoft updates. Of the approximately 8,000 NIPR workstations that needed to be patched following "patch Tuesday," it was common for less than 1% of information systems to need manual remediation due to a failure of the WSUS or Windows Update Agent (WUA). Unfortunately, CPT Sabovich had no automated system capable of deploying third-party updates. As a result, he relied on batch files and visual

[84] Czumak III, "Recommendations for a Standardized Program Management Office (PMO) Time Compliance Network Order (TCNO) Patching Process."

basic scripts to deploy third-party patches to thousands of computers on a monthly basis. While these methods were often successful, they were also extremely time consuming and could only patch computers online at the time the script attempted to ping[85] a computer. Patching using scripts does not allow for retries when computers are offline at the time the script is executed.

In 2007 to 2008, the Theater Network Operations Center (TNOSC) for the U.S. Army Pacific (USARPAC) was using Altiris[86] to deploy software packages, including third-party updates. Using Altiris to deploy patches required that every third-party vulnerability had to have a special update package made to patch the vulnerability. This manual process was labor intensive and prone to error. In addition, Altiris was deployed with the TNOSC as the top tier of the server architecture because Altiris had not been adopted as an enterprise solution, and was only a theater level solution for the Pacific. Thus, the Altiris section at the TNOSC became responsible for creating all software update packages, including third-party updates, which was under manned and over allocated to other tasks in addition to Altiris management. In practice, due to oversight or human error, update packages were often forgotten. This type of problem was noted by Ross, Weill and Robertson who found in their book, *Enterprise Architecture as Strategy*, that automation of routine activities was essential for tasks to be completed reliably and predictably.[87] They found that organizations that had perfected routine activities had more time and energy to devote to excellence. Unfortunately, the DoD's solution to standardize third-party vulnerability remediation was the Secure Configuration Remediation Initiative (SCRI), also known as Citadel Hercules. As mentioned earlier, the

[85] The Packet Internet Groper or PING command is used by system administrators to determine if a system is reachable before attempting to send an update package with a script.

[86] Altiris is a software inventory and deployment solution that allows for custom software applications or patches to be remotely deployed and installed on any Windows information system that is running an Altiris Client.

[87] Jeanne W. Ross, Peter Weill, and David Robertson, *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution* (Boston, MA: Harvard Business School Press, 2006), 3.

Army CIO/G-6 was unhappy with Hercules and instead elected to standardize Microsoft SMS as the enterprise solution.[88]

Hercules was never fielded to individual components of the Army, such as USARPAC. The software was provided for download, but Army units were left trying to secure the funding necessary to field the additional servers required to operate Hercules. Units were also left with the task of installing and configuring Hercules and then training soldiers to operate it. The result was that a small number of commands implemented Hercules, but found the results were less than favorable. Word spread throughout the Army IA community that Hercules was a poor product with numerous problems. In September 2010, the Army Enterprise-Wide Steering Group (ESSG) voted to discontinue funding for SCRI due to "the lack of usage from the Combatant Commands Services, and Agencies (CC/S/A's) regarding the SCRI capability."[89]

By 2008, the Army still employed a varied collection of vulnerability management solutions aimed at addressing third-party vulnerabilities. An example was the scripting solutions CPT Sabovich deployed as the NOSC chief. At the time, CPT Sabovich had personal knowledge of several other NOSCs employing similar techniques he was using, in an attempt to address the lack of third-party automated patching capability. Other commands had turned to third-party vendors, such as Altiris, BigFix, Shavlik, ScriptLogic and SolarWinds, to name a few of the more popular options. Each of these was a stove-piped automated patching solution that may have been effective at applying Microsoft and third-party patches, but failed to offer a unified architecture for remediating application vulnerabilities. That is not to say that the above solutions could not scale to support the Army vulnerability management needs; some of them could. Unfortunately, they were implemented at the bottom to mid-level of the enterprise that prevented a coherent enterprise architecture from being implemented. In essence, these

---

[88] Tim Ash, and Mike Spragg, "NetOps Implementation Update (CMDB, SMS/MOM, SCTS.)," *U.S. Army Network Enterprise Technology Command*, August 22, 2007, www.afcea.org/events/pastevents/documents/Track4Session5-NetOpsUpdate.ppt, 12.

[89] Defense Information Systems Agency, "Termination of Secure Configuration Remediation Initiative (SCRI) Support," September 2010, http://iase.disa.mil/tools/disa_termination_of_scri_support.doc.

solutions were all implemented in isolation of each other, usually at the NOSC level, or at best, at the TNOSC level.

In March 2009, NETCOM was assigned as the sole IT service provider for the Army. As part of this new mission, NETCOM was given the lead on a new initiative to transform the LWN.[90] The new initiative was and currently still is known as the Global Network Enterprise Construct 6+1 (GNEC) and represents a unified effort by the Army to create enterprise-wide standardization across the Army's portion of the GIG. Part of the standardization effort was directed at fielding a comprehensive vulnerability management solution to the LWN.

In an effort to deploy SMS enterprise wide successfully, the Army engaged Microsoft Consulting Services (MCS) to architect a plan for the fielding. The Army assigned the name of SysMan to the two products selected by Microsoft to meet the requirements of the Army. SysMan consists of SCCM and SCOM 2007. SCCM was built using the WSUS framework as a starting point, and in addition to Microsoft updates, it can deploy software packages, complete operating systems, perform software and hardware inventory, and perform CM.[91] With the addition of the SCUP add-in, SCCM can also deploy third-party updates. WSUS servers are authorized for continued use, but only in support of SCCM. SCCM 2007 retains most of the same Microsoft software update capabilities as a standalone WSUS, because SCCM maintains control of its own internal WSUS.[92] Due to the way SCCM controls WSUS, automatic approval and deployment of updates is not supported by SCCM. System administrators must manually deploy updates to specified collections of computers.

The Army also fielded SCCM with the Quest Xtensions Manager (QXM) module, which allows SCCM to manage non-Windows based devices, including information systems using operating systems from Linux, Unix, Mac, Cisco and others by deploying a

---

[90] Barry Rosenberg, "NETCOM, GNEC Directives Transform Army LandWarNet—Defense Systems," *Defense Systems*, November 13, 2009, http://defensesystems.com/articles/2009/11/18/c4isr-lawrence-army-network-enterprise-technology-command.aspx.

[91] Microsoft, "System Center Configuration Manager Overview," August, 2011, http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-overview.aspx.

[92] Ibid.

separate software agent to each non-Microsoft system.[93] The use of this is significant, because although the Army's client environment is overwhelmingly Windows based, it does use a limited number of non-Windows operating systems in its server environment. Microsoft claims that over 95% of Army information systems are based on Microsoft technologies.[94]

The second part of SysMan, SCOM, is primarily an end-to-end service monitoring tool. SCOM is typically used to monitor the status of key business services, such as the status of company websites, databases, exchange servers or active directory servers.[95] As such, SCOM has little to do with performing patching, beyond monitoring the status of SCCM or WSUS servers.

Unfortunately mitigating third-party application vulnerabilities with SCCM can be problematic. The first problem with SCCM 2007 is its scalability. A single hierarchy can support up to 200,000 clients using primary and secondary sites. Each primary site supports up to 100,000 clients, and each primary site can have child primary sites. Considering the Army has over 700,000 desktops and 20,000 servers, a minimum of four hierarchies are mandatory.[96] To address this problem, the Army chose to implement 10 SCCM hierarchies, along with two custom extensions.[97] The first extension is an Enterprise Package Repository, which is a file server that interfaces with each of the 10 central sites in the hierarchy to provide software packages. The second extension is an Enterprise Data Warehouse, which collects reporting data from each of the 10 SCCM central sites. These two extensions provide an effective workaround for the scalability problems of SCCM and allow the NETCOM package team to create and distribute

---

[93] Quest Software, "Quest Management Xtensions—Configuration Manager," 2011, http://www.quest.com/quest-management-xtensions-device-management-CM/.

[94] Microsoft, *Performance Work Statement For United States Army Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM/9th SC (A)), Enterprise Systems Technology Activity (ETSA) For Microsoft Consulting Services For Systems Management (SysMan) Sustainment Support*, Microsoft, July 13, 2009.

[95] Microsoft, "End to End Service Monitoring With Microsoft System Center Operations Manager 2007," *Microsoft TechNet*, 2007, http://technet.microsoft.com/en-us/systemcenter/om/bb498233.

[96] U.S. Army Network Enterprise Technology Command, "ConfigMgr 2007 Enterprise Architecture: SysMan," *NETCOM*, January 26, 2009, 6.

[97] Ibid., 28.

software packages, to include third-party updates, to each of the central sites in the hierarchy, from one central point.[98] These extensions represent custom work by Microsoft Consulting Services and are not available in a typical SCCM deployment. This hierarchy requires that each central site (TNOSC level) host a minimum of five servers to support up to 100,000 clients, or four servers to support 60,000 clients. At tier 2 (NOSC level), each site requires at least 11 servers to support up to 15,000 clients because each SCCM Distribution Point (DP) server supports up to 2,000 clients.[99] Figure 14 shows a very basic diagram of the Army's current SCCM deployment. Supporting a deployment of this magnitude requires a dedicated team of specialists from Microsoft.

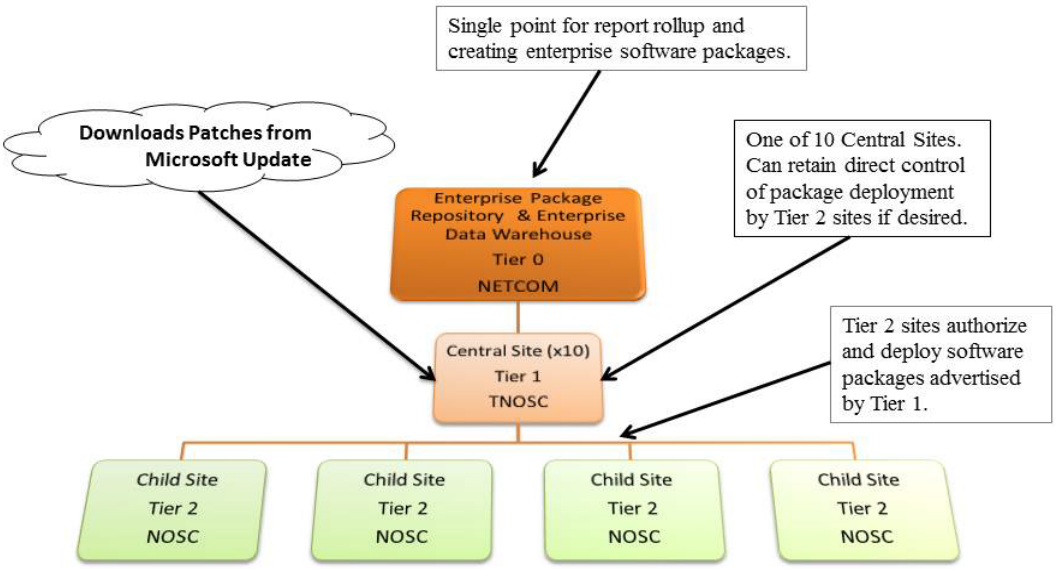


Figure 14. Current Army SCCM 2007 Deployment Architecture[100]

Another shortcoming of SCCM is that it still requires the system administrator to create special update packages when a new third-party patch is released. A case study by Shavlik Technologies found that SCCM requires administrators to create a deployment package for each individual third-party patch. This process took approximately two hours

[98] U.S. Army Network Enterprise Technology Command, "ConfigMgr 2007 Enterprise Architecture: SysMan," 78–79.

[99] Ibid., 32–36.

[100] Ibid.

per patch and is separate from the Microsoft patch deployment done by SCCM or WSUS.[101] As a best case scenario, an additional burden is created on administrators at the top tier of the network where SCCM is deployed. In the worst case scenario, system administrators at Tier 0 forget to create or deploy patch packages, which leaves information systems needlessly vulnerable.

A further limitation with SCCM implementation is that the top level WSUS portion of SCCM has to sync with the Microsoft's update server.[102] As the U.S. Army's deployment of SCCM uses 10 top level sites, each tier 1 central site must sync directly from Microsoft Update servers, instead of having the option of pulling updates from, perhaps, a single DoD master server. Child SCCM servers can still inherit update packages authorized by their parent SCCM server, which eases the burden of subordinate SCCM administrators having to recreate software packages already created by their parent SCCM server.

Another shortcoming of SCCM is the complexity of the system. The U.S. Army provides a one-week, 40-hour course. However, industry experts suggest that being a competent SCCM administrator takes in excess of one year of experience or training. The average soldier in the Army is often only in one duty position for 12–18 months, and as a result, they do not have the luxury of an extended time period to learn to be effective with the tools of their trade, which is especially true at the NOSC level, where soldiers rotate frequently. It is less of an issue at the TNOSC and NETCOM level because of their reliance on DA civilians and contractors, who tend to hold their positions longer. Still, reliance on contractors to operate NetOps tools can present a problem. CPT Sabovich experienced this firsthand, when in 2009, the current TNOSC contractors did not win their contract renewal. An almost completely new group of contractors arrived at the TNOSC to takeover NetOps. Not surprisingly, the outgoing contractors were not highly

---

[101] Shavlik, "Case Study: Harbor One Credit Union," *Shavlik Technologies*, 2011, http://www.shavlik.com/assets/docs/cs-harborone-credit-union.pdf.

[102] David Dixon, "SCCM\WSUS—Streaming from an Upstream Server," *Microsoft TechNet*, May 14, 2009, http://blogs.technet.com/b/daviddixon/archive/2009/05/14/sccm-wsus-streaming-from-an-upstream-server.aspx.

motivated to provide continuity of operations, which resulted in the TNOSC providing poor service while the new contractors attempted to learn their jobs.

Despite some shortcomings, Microsoft SCCM does possess many advantages, including a wide range of capabilities, a large amount of custom add-ons from third-party vendors, a large customer base and the support of Microsoft, which invented the CM business for Windows computers. Bowens reported in the *Army Communicator* in 2010 that both Fort Rucker and Fort Monroe used SCCM to deploy the newly mandated Microsoft Vista OS. Information Management Officers (IMOs) at Fort Rucker conceded that it took them over a year develop a process that allowed SCCM to automate the deployment of Microsoft Vista, while keeping the user profile intact. IMOs at Fort Rucker were also successfully using SCCM to deploy patches and make configuration changes.[103] Both Fort Rucker and Fort Monroe operate at Tier 2 of the SCCM architecture, which allows them to sync to their Tier 1 SCCM parent server, the CONUS TNOSC (CTNOSC). The CTNOSC, in turn, syncs to the Tier 0 EPR and EDW run by NETCOM, which moves the burden of patch and software package creation away from the TNOSCs at Tier 1 and the NOSCs at Tier 2 and centralizes it with NETCOM at Tier 0. As long as Tier 0 does their job, the TNOSC and NOSC SCCM servers will download software packages, including Microsoft updates and custom updates (including third-party patches created with SCUP[104]) automatically. Once completed, it is up to the TNOSCs and NOSCs to create jobs to deploy the software and updates.

The fielding of SCCM to all required organizations in the Army has proven to be very time consuming and is still a work in progress. A deadline of December 31, 2011 was set by ARCYBER for all Army organizations on the NIPR/SIPR networks to transition to SCCM.[105] As of February 2012, approximately 75% of the NIPRNET had

---

[103] Roland Bowens, "Fort Rucker, Fort Monroe Etch an NEC Success Story," *Army Communicator*, Fall 2010, http://findarticles.com/p/articles/mi_m0PAA/is_3_35/ai_n56745408/, 22.

[104] SCUP—Microsoft System Center Update Publisher allows for the custom third-party software patches to be imported into SCCM, which will then treat the third-party patch as if it were a Microsoft update.

[105] Alice Connor, *U.S. Army Cyber Command Execute Order (EXORD) 2011-090 Implementation and Integration of System Center Configuration Management (SCCM) and NIPRNET and SIPRNET*, U.S. Army Cyber Command, Fort Belvoir, VA, September 20, 2011.

been fielded SCCM, including all of the TNOSCs.[106] It is not surprising that many organizations were unable to make the deadline due to the inherent challenges and complexity of deploying and implementing SCCM. Other major software and hardware deployments, such as the Army's migration to Windows Vista in 2008–2009, also missed their deadlines, but eventually neared 100% compliance. It is reasonable to assume that SCCM compliance rates will reach into the mid to high 90% range given its emphasis from NETCOM leadership.

To date, the Army's tactical networks have not been widely fielded with SCCM. The fielding of SCCM did not coincide with the acquisitions cycle that tactical networks were under when SCCM was originally contracted. As a result, tactical networks continue to rely heavily on their WSUS to deploy Microsoft patches. A small number of tactical units have been fielded with SCCM, but the majority is still operating without it. The intent of the ARCYBER is to field SCCM to all tactical units; however, it is unclear when this will be done, as the deadline for full compliance has already passed. In comparison to garrison networks, tactical networks pose several unique challenges for an automated patching solution.

The first and most significant challenge that any vulnerability management solution faces on tactical networks is a lack of bandwidth. Typically, a Brigade Combat Teams (BCT) G6 section operates and maintains the enterprise services for the BCT. These enterprise services are housed in the Battle Command Common Services (BCCS) server stack. The BCCS stack is currently on its fourth revision, and in conjunction with SCCM fielding, tactical units are also receiving VMware ESX virtualized servers to host their enterprise services.[107] Enterprise services in the BCCS stack generally mirror those of found at a TNOSC, including Microsoft AD, DNS, DHCP, Exchange, SharePoint, HBSS, anti-virus, Retina, SCCM/WSUS and others. In the field, a BCT normally has 16 Mbps connection to each of its battalions via the High Capacity Line of Sight (HCLOS)

[106] Personal correspondence with U.S. Army Network Enterprise Technology Command official on February 3, 2012.

[107] George L. Seffers, "Improved Cloud over the Horizon for Warfighters," *Signal Online*, November 10, 2011, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2795&zoneid=333.

radios and 7 Mbps combined satellite bandwidth for the entire BCT.[108] Satellite bandwidth allocations can be increased for each BCT to meet mission requirements as long as funding/satellite capacity is available. The HCLOS and satellite communications also support both SIPR and NIPR networks, meaning that for a BCT, bandwidth is always at a premium.[109] The implications of patching in a low bandwidth environment are obvious. Patching windows must be managed very carefully so that the network is not saturated with update traffic. In a garrison environment, this saturation is typically not much of an issue as workstations tend to occupy the same Local Area Network (LAN) segment as the update servers, which provides each workstation between 100Mpbs to 1Gbps of bandwidth.

Another limitation that any vulnerability management solution faces while operating in a tactical environment is the infrequent level of client connection to the network. Often clients will reside off the network for days, only to connect to the network for a short period before disconnecting again, which poses unique challenges for a patching solution because of the small window of time available to patch clients. In the tactical environment, agent-based patching tools offer the best solution for patching remote clients because each client can be configured to check-in with the patching tool upon authenticating to the network. At this time, the patching tool can check the client for missing patches and remediate as necessary. If an agentless solution was utilized, only clients authenticated to the network at the time of patch deployment could be remediated. Invariably, many clients would be missed and thus require multiple iterations of patch deployment, which is very inefficient for system administrators.

The process that the Army currently uses to manage the remediation of the tremendous numbers of vulnerabilities reported on a daily basis from both the public and private sectors is known as the Information Assurance Vulnerability Management (IAVM) Process.

---

[108] Headquarters, Department of the Army, *FM 6-02.60, Tactics Techniques and Procedures (TTPs) for the Joint Network Node—Network (JNN-N)*, U.S. Army Training and Doctrine Command, 2006, https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fmi6_02x60.pdf.

[109] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE ARMY INFORMATION ASSURANCE VULNERABILITY MANAGEMENT PROCESS

A. THE IAVM PROCESS

The IAVM process is how the DoD and the U.S. Army manage the risk posed by the tremendous number of new software and configuration flaws discovered by good intentioned researchers and cyber criminals alike. The IAVM process sets the minimum security standard for an information system to operate on a U.S. Army network. Army Regulation 25-2 describes the desired end state of the Army IAVM process as "a proactive methodology of maintaining, patching and updating systems before notification or exploitation."[110] DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, explains that the DoD IAVM process "provides positive control over the vulnerability notification process for DoD network assets."[111] The process requires each component to acknowledge the receipt of an IAVM message, and it sets deadlines for implementing the countermeasures described in the IAVM. The IAVM process consists of four phases.

1. Vulnerability identification, dissemination, and acknowledgement
2. Application of measures to affected systems to bring them into compliance
3. Compliance reporting
4. Compliance verification

Vulnerability identification can begin at the DoD level, but it is usually initiated when a software or configuration flaw is reported to the vendor of the hardware/software compromised. The vulnerability enters the DoD reporting chain with USCYBERCOM.[112] USCYBERCOM is responsible for disseminating IAVM messages

[110] Headquarters, Department of the Army, *AR 25-2, Information Assurance* (Washington, DC: U.S. Army Training and Doctrine Command, 2009), http://armypubs.army.mil/epubs/pdf/r25_2.pdf, 44.

[111] U.S. Secretary of Defense, Information Assurance Workforce Improvement Program (DoD 8570.1M), Department of Defense, 2005, http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf, 86.

[112] U.S. Cyber Command is responsible joint cyberspace operations in the DoD. USCYBERCOM absorbed Joint Task Force Global Network Operations (JTF-GNO), as well as the Joint Functional Command—Network Warfare (JFCC-NW). Full operational capability was reached by USCYBERCOM on October 31, 2010. Prior to USCYBERCOM, JTF-GNO released all IAVM messages.

to each of the service components for acknowledgement and action. The service components consist of ARCYBER/2nd Army, Fleet Cyber Command/10th Fleet, Air Forces Cyber/24th Air Force and Marine Corps Forces Cyberspace Command, as depicted in Figure 15.[113]

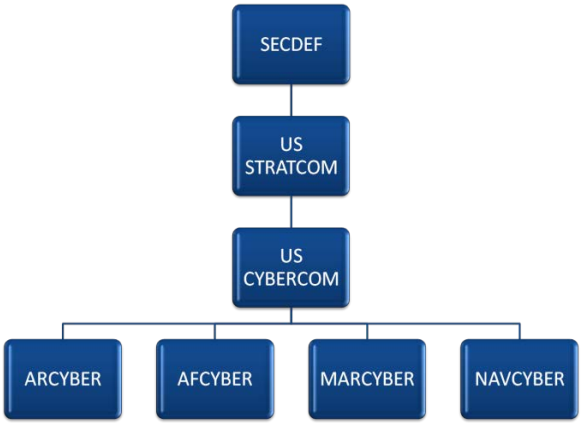
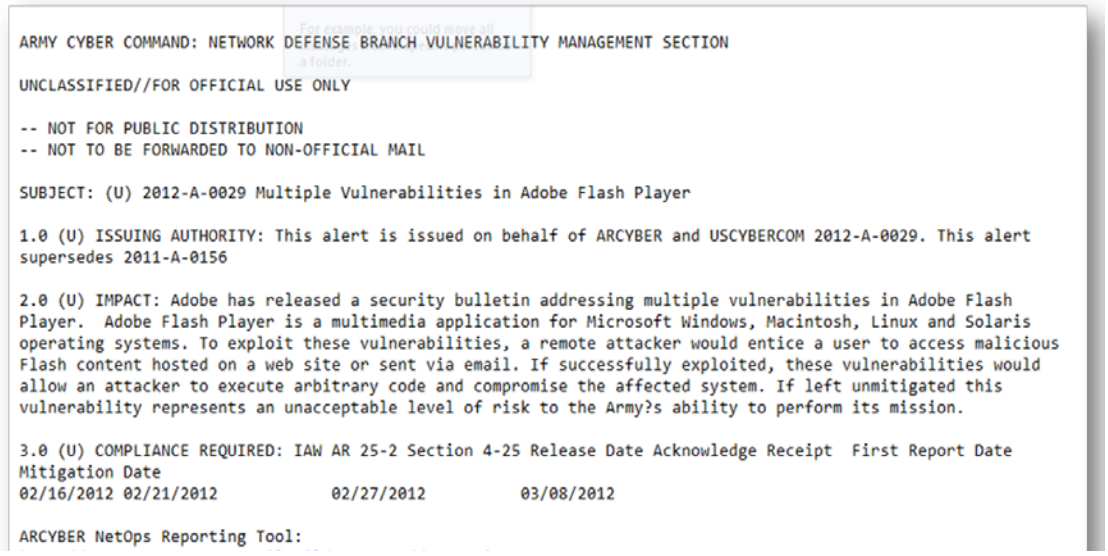


Figure 15. Command Structure: SECDEF to ARCYBER

Before the IAVM message is sent, it is categorized as an Information Assurance Vulnerability Alert (IAVA), an Information Assurance Vulnerability Bulletin (IAVB), or an Information Assurance Technical Tip (IATT). The IAVA is the most severe of the IAVM messages, and requires acknowledgement, as shown in Figure 16. It also specifies the date that the remediation action must be completed and reported up the chain of command. The IAVB requires acknowledgment as well, but allows commands to implement corrective actions as time allows.

[113] Wikipedia, "United States Cyber Command," February 17, 2012, http://en.wikipedia.org/wiki/United_States_Cyber_Command.



ARMY CYBER COMMAND: NETWORK DEFENSE BRANCH VULNERABILITY MANAGEMENT SECTION

UNCLASSIFIED//FOR OFFICIAL USE ONLY

-- NOT FOR PUBLIC DISTRIBUTION
-- NOT TO BE FORWARDED TO NON-OFFICIAL MAIL

SUBJECT: (U) 2012-A-0029 Multiple Vulnerabilities in Adobe Flash Player

1.0 (U) ISSUING AUTHORITY: This alert is issued on behalf of ARCYBER and USCYBERCOM 2012-A-0029. This alert supersedes 2011-A-0156

2.0 (U) IMPACT: Adobe has released a security bulletin addressing multiple vulnerabilities in Adobe Flash Player. Adobe Flash Player is a multimedia application for Microsoft Windows, Macintosh, Linux and Solaris operating systems. To exploit these vulnerabilities, a remote attacker would entice a user to access malicious Flash content hosted on a web site or sent via email. If successfully exploited, these vulnerabilities would allow an attacker to execute arbitrary code and compromise the affected system. If left unmitigated this vulnerability represents an unacceptable level of risk to the Army?s ability to perform its mission.

3.0 (U) COMPLIANCE REQUIRED: IAW AR 25-2 Section 4-25 Release Date Acknowledge Receipt First Report Date Mitigation Date
02/16/2012 02/21/2012 02/27/2012 03/08/2012

ARCYBER NetOps Reporting Tool:

Figure 16. Excerpt from Adobe Flash Player IAVA Message[114]

Remediation action of the IAVB is required, but not reported. IATTs are vulnerabilities that represent the least danger to the LWN and do not require acknowledgement of receipt or a report of completion. Commands are still required to complete the remediation action, however.[115]

IAVMs are disseminated in parallel from ARCYBER to NETCOM, and to each Signal Command, TNOSC and NOSC. Currently, the LWN is controlled by four separate signal commands, as depicted in Figure 17. The largest is the 7th Signal Command (Theater), which is responsible for the CONUS TNOSC (C-TNOSC) and all 14 subordinate CONUS-based NECs/NOSCs. The 7th SC(T) controls 84% of Army network assets, more than double all other signal commands combined.[116] Army networks in Europe are the responsibility of the 5th Signal Command (Theater), which controls the Europe TNOSC (E-TNOSC). The 311th Signal Command (Theater) is responsible for the Pacific region and controls the Pacific TNOSC (P-TNOSC) and the Korea TNOSC (K-

[114] Army Cyber Command., "2012-A-0029 Multiple Vulnerabilities in Adobe Flash Player," *ARCYBER*, February, 2012.

[115] Headquarters, Department of the Army, *AR 25-2, Information Assurance*, 44.

[116] G3 7th SC(T), "7th Signal Command Theater: One Team One Network," *Armed Forces Communications and Electronics Association*, September 30, 2009, http://www.afcea-augusta.org/industry_day_slides/day1/7th_Sig_Industry_Day_Brief_(releasable).pdf.

TNOSC). Finally, the 335th Signal Command is responsible for the CENTCOM AOR, including Iraq and Afghanistan and operates the South West Asia TNOSC (SWA-TNOSC).[117]

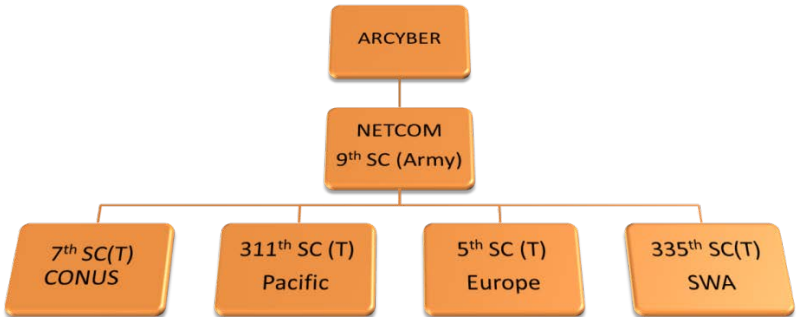


Figure 17. Command Structure: ARCYBER to SC(T)

Each SC(T) forwards the IAVM received from ARCYBER to its respective TNOSCs for action. The TNOSC or subordinate NOC/NOSC (in the case of the 7th SC(T)) is the element of each SC(T) that contains the expertise and information systems necessary to implement the directives in the IAVMs for its respective geographic areas. Each TNOSC normally modifies the IAVM sent by ARCYBER to reflect suspense dates for actions necessary that are one to two days prior to the ARCYBER suspense. Once the IAVM is sent by each TNOSC to its respective NOSCs, the NOSCs acknowledge receipt of the message and initiate corrective actions on their portions of the network to meet the suspense of the TNOSC and ARCYBER. NOSCs do not have to wait for an IAVM message to begin remediating known vulnerabilities.

Each TNOSC controls the enterprise tools and services for its theater. At a minimum, it consists of DMZ IA devices, Microsoft AD domain controllers, Microsoft Exchange e-mail servers, Symantec Anti-Virus servers, DNS servers, Domain Host Configuration Protocol (DHCP) servers, Spectrum Network Management servers, Retina vulnerability scanning servers, Remedy servers and SCCM/SCOM servers. Each TNOSC is functionally organized, with a team of Subject Matter Experts (SME) tasked to manage

[117] Army Reserve, "335th Signal Command Theater," *United States Army Reserve*, (n.d.), http://www.usar.army.mil/arweb/organization/commandstructure/USARC/OPS/335Sig/Pages/default.aspx.

the operation of each functional area. The TNOSC IA team uses the eEye Retina Network Security Scanner (NSS) to assess the vulnerability level of its network. Another team in the TNOSC manages the SCCM/SCOM servers.

The NOSCs that operate below the TNOSCs do not have the same level of manning, nor do they generally have the expertise to operate the enterprise tools that the TNOSC controls. The NOSC is also responsible for a much smaller geographic area than the TNOSC. An example is the 311th Signal command, which is a subordinate command of USARPAC. The 311th SC controls the P-TNOSC and K-TNOSC, which together exercise control over five geographic areas in the Pacific, which consists of the Hawaiian Islands, Alaska, Okinawa, Japan and Korea (Figure 18). One signal battalion/NEC and its associated NOSC control one geographic region. For example, the 30th Signal Battalion/NEC and its NOSC controls the Army portion of the LWN for the Hawaiian Islands.

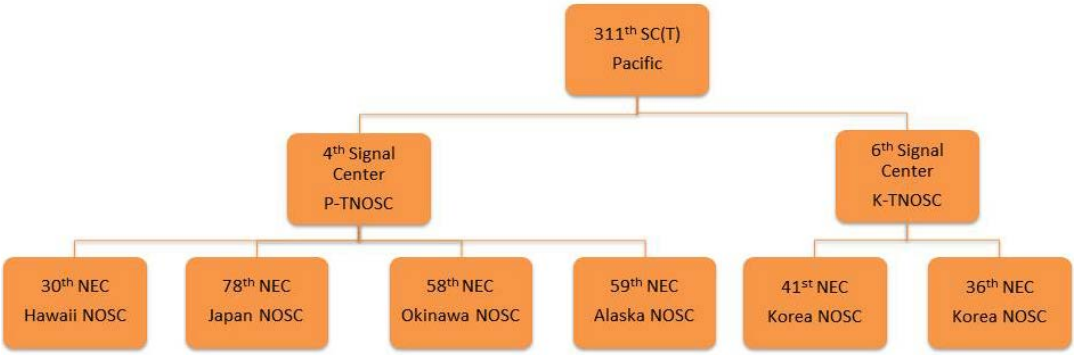


Figure 18. Functional Organization of the 311th Signal Command for IAVM Reporting

Each TNOSC can allow its regional NOSCs to control elements of the enterprise tools, at its discretion. Normally, NOSCs have AD control of their AD Organization Units (OUs). They are also provided eEye Retina servers to scan their segments of the network and are provided with administrative access to their WSUS or SCCM/SCOM servers. This control is important because each NOSC has a direct working relationship with each of their supported units. The TNOSC does not normally know all the special

needs of each unit in a region like a NOSC does. As a result, the NOSC should know what information systems are program managed, and do not receive automatic updates. Upon receiving an IAVM, NETCOM, TNOSC and NOC/NOSC technicians will turn to their network scanners and automated tools to comply with the IAVM.

B. VULNERABILITY SCANNING

ARCYBER and subordinate units operate the eEye Retina network security scanner and the Remote Enterprise Manager (REM) security management console, under the DoD initiative known as the Secure Configuration Compliance Validation Initiative (SCCVI). SCCVI included a DoD-wide acquisition for REM and Retina, provided an Enterprise License Agreement (ELA) for REM and Retina, and training at no cost to the services.[118] Both of these tools are included under GNEC 6+1, as shown in Figure 19. The retina scanner searches for software and configuration vulnerabilities. Vulnerability scans are run by hostname, IP address list, IP address range or subnet and can search for all known vulnerabilities, or from a specific list, such as all IAVAs. Scans are normally tailored as much as possible by IP address range and vulnerability type because it reduces the amount of time it takes to complete a scan. Scanning is not a trivial task; completing a scan of several thousand computers can take the better part of a day, and it increases network congestion. The greater the number of vulnerabilities selected in a scan, the longer the scan takes to complete. As a result, scans normally target only active IAVMs. Once a scan is completed, a report is generated by Retina that can be viewed in either a web browser or Microsoft Excel. This report is then parsed by vulnerability type (either CVE[119] number, or IAVA, IAVB, IAVM) and assigned a remediation task.

[118] Ash and Spragg, "NetOps Implementation Update (CMDB, SMS/MOM, SCTS)."

[119] CVE refers to the Common Vulnerability and Exposures number, which is a unique number assigned to all publically known information security vulnerabilities.

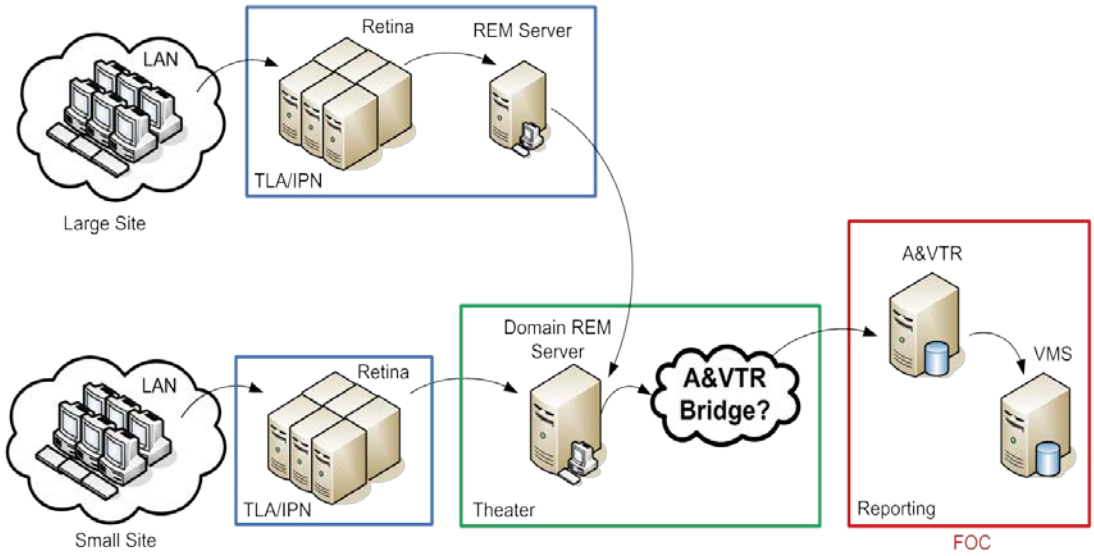


Figure 19. REM/Retina Logical Architecture[120]

The results of the retina scans completed by the NOSCs/NOCs are consolidated at the Tier 1 TNOSC REM server, before being aggregated into an Army IT Asset Management (ITAM) Extensible Markup Language (XML) database run by the Defense Information Systems Agency (DISA).[121] REM data, along with information from other data sources, including SCCM, McAfee HBSS ePO, and Computer Associates IT Client Manager, is then synthesized for viewing by authorized users over web browsers. In the past, vulnerability compliance reports were generated at the NOSC level, and manually forwarded by e-mail to the TNOSC and were then manually consolidated by the TNOSC and forwarded to the AGNOC (now ARCYBER). In other words, anytime vulnerability reporting information was needed, a data call had to be initiated. The result was a time consuming process that became more difficult to complete as the number of reporting units increased. With the new system, authorized users are still dependent on the NOSCs/TNOSCs to complete scanning, but they do not have to wait for data call

[120] NETCOM, "NetOps Implementation Update: SCCVI Employment (eEye Retina / Remote Enterprise Manager)."

[121] Elizabeth Floyd, Benita Vailoff, and Tom Stuckey, "IT Asset Management: Information Exchange Forum Session: 2," Proceedings from the LandWarNet Conference, *Armed Forces Communications and Electronics Association*, April 2011, http://www.afcea.org/events/pastevents/documents/LWN11_ITAM_Session_2.pdf.

completion to view useful data as the ITAM database contains the most current scan data for each region. Remediation of the vulnerabilities verified using REM/Retina relies primarily on Microsoft SCCM 2007.

C. AUTOMATED REMEDIATION OF IAVMS FOR MICROSOFT VULNERABILITIES

When an IAVM is received by NETCOM G5 section from ARCYBER, analysts determine what deployment packages are needed to create for their Tier 0 EPR server. IAVM messages can arrive at any time of the month, however, patch Tuesday[122] normally produces the highest volume of updates for the month, as Microsoft generally releases more updates per month than any other single vendor. The updates needed for patch Tuesday are also the easiest to create, as the patches and their associated metadata are supplied directly from Microsoft. Due to the hierarchy employed by the U.S. Army with SCCM 2007, NETCOM Tier 0 technicians do not download or approve any Microsoft updates because the first tier of SCCM servers are operated at the TNOSC level.

System administrators operating the TNOSC Tier 1 SCCM servers then authorize their SCCM servers to download the appropriate patches from Microsoft to address the new vulnerabilities. The actual download and authorization of the updates is done by WSUS server(s), known as Software Update Points (SUP), which operate under the direct control of SCCM. Once the updates are downloaded, the TNOSC may elect to test the updates in a lab environment, although this often is seldom used when deploying Microsoft updates. Following testing, the TNOSC has the option of creating device collections and deploying updates to Tier 2 sites. Alternatively, they can advertise the Microsoft updates to their Tier 2 child sites and allow Tier 2 system administrators to locally control of update deployment. If the Tier 2 site is given control update deployment, they then manually specify what client collection will receive each update, and apply specific deployment rules. SCCM contains an inventory function that shows all computers that report to SCCM, along with any Microsoft updates needed. At the NOSC

[122] Patch Tuesday refers to the second Tuesday of every month, which is Microsoft's release date for all new patches made to address vulnerabilities discovered since the last release cycle.

and TNOSC level, certain computers that are program managed or of high importance (including most servers) are left to the system owners to update manually. This precaution is taken to ensure that non-standard applications, which are not covered under the AGM program, are not impacted by the automated updates. The remainder of the computer inventory is then scheduled to receive the updates.

Updating schedules vary by region. Deploying patches during working hours ensures that that most computers are online and available updates. The downside of this method is that regular work hours are when the network is at its highest bandwidth utilization. Depending on the capacity of each site, deploying patches during the day may cause an unacceptable degradation in network performance and disruption to system users. Patch deployment during non-business hours, including the weekends, is another option. Nearly all commands have some form of energy conservation policy that stipulates that all non-mission essential computers and office automation will be powered down at the end of the duty day, which limits the effectiveness of deploying patches during off-duty times, but it has the advantage of preventing patching from impacting network performance. In practice, most organizations are forced to deploy patches during the day and then schedule a reboot in the evenings for computers left powered on. Microsoft SCCM keeps track of offline computers during patch deployment and will attempt to install the updates once the computers come online.[123] Additionally, SCCM can attempt to use Wake on LAN (WoL) to power on computers turned off for the day.[124]

Invariably, some computers cannot be updated by SCCM because of various problems, including a lack of hard disk space, a corrupt SCCM agent or numerous other potential issues. Often NOSCs will elect to do a clean install with the latest AGM image instead of spending time troubleshooting client problems with automatic patching. Automated deployment of AGM images is another capability of SCCM, which several Army units have used successfully.[125] If clients cannot be remediated, depending on local

[123] Microsoft, "System Center Configuration Manager Overview," 2.

[124] Ibid., 2.

[125] Bowens, "Fort Rucker, Fort Monroe Etch an NEC Success Story."

NOSC/TNOSC policy, they are then blocked from network access, and/or disabled and moved to a "mitigation" OU in AD. Once the local system administrator for the quarantined computer applies patches, it is re-scanned by the NOSC IA team and verified to meet IAVM requirements. The final step is unblocking the computer and moving it back to its original OU.

D. AUTOMATED REMEDIATION OF IAVMS FOR THIRD-PARTY VULNERABILITIES

Deployment of third-party updates follows the same general process as Microsoft updates, but because SCCM does not natively support third-party updates, additional steps are required for SCCM to deploy these patches. The first step that the NETCOM G5 section takes upon receipt of an IAVM is to review the SCUP update catalog, which is done to determine if the third-party vendor identified in the IAVM has supplied Microsoft with an entry into the custom update catalog. Currently, Dell, Hewlett Packard and Adobe provide custom updates to Microsoft for inclusion with the SCUP tool. Adobe only provides SCUP support for its Reader, Flash and Acrobat products. Dell and HP both provide automated BIOS, firmware, driver, and vendor specific application updates.[126] If the updates are available from the SCUP custom update catalog, the update package is imported using SCUP into SCCM and published. Once the update is published to SCCM, it becomes available for deployment, like any Microsoft update.

If the update is not in the Microsoft catalog, the NETCOM team must create the update package from scratch. For a typical patch, such as deploying a new version of Sun Java, several steps are involved. The first step is to acquire the executable file from the third-party vendor. Ideally, an .msi file should be used as a starting point for creating a custom update, because it contains built-in detection logic for deployment. Normal .exe files contain no detection logic, and as such, require more work for the system administrator. If an .exe file was used as the basis for creating the update, the NETCOM team needs to research which command line switches to use to install the patch silently without user involvement. Each vendor uses a separate set of command line switches for

[126] Microsoft, "Third-Party Custom Catalogs for Configuration Manager 2007 and System Center Essentials 2007," 2012, http://technet.microsoft.com/en-us/systemcenter/cm/bb892875.aspx.

the unattended installation of its patches. Next, the team must specify the detection logic for installation. In this situation, retina scans are useful because each vulnerability has a signature that Retina uses for detection, which is normally a registry key or file name that when found, alerts Retina that a specific vulnerability exists. The same detection logic can then be applied in creating the new patch. After detection logic is applied using SCUP, the update package is created and published to SCCM. It will be necessary to create an update package for each vulnerable operating system to include different versions of Windows and each server OS. In the case of Sun Java, the NETCOM team would also run a silent uninstall of any old versions of Java found on the computer. If this step is missed, Retina will continue to report computers that have been patched as vulnerable. Finding the registry keys to uninstall old versions of applications can be very time consuming. After all these steps are completed, the G5 team will proceed with testing to ensure the update package functions properly in a test environment. If testing is successful, the G5 team will upload the package to its EPR server. The EPR server copies each package to the source directory of each Tier 1 central site.[127] The remainder of the patching process mirrors that of Microsoft updates. This process works, but it is far from optimal. The next section discusses several of the most significant challenges facing the IAVM process, specifically in regards to patching third-party applications.

E. PROBLEMS WITH THE CURRENT PROCESS

The single largest problem with the current IAVM process is that the Army's chosen solution for patching and CM, SCCM 2007 has taken far too long to reach all of the organizations that need it. It is beyond the scope of this thesis to determine exactly why it has taken so long; however, the complexity of SCCM almost certainly played a central role in delaying the deployment. The fact remains that after over five years of fielding, large segments of the Army's four networks are still untouched by SCCM. As a result, many organizations that need an effective enterprise provided third-party patching tool are either using locally procured solutions, scripts, manual updating, or ignoring third-party updates. A lightweight third-party patching solution that utilized either

[127] U.S. Army Network Enterprise Technology Command, "ConfigMgr 2007 Enterprise Architecture: SysMan," 78.

existing server architecture or had a very small footprint could potentially have been fielded much faster than SCCM. It is also very likely that a lightweight solution would not provide the same breadth of capabilities that SCCM does.

Little argument exists that Microsoft SCCM 2007 provides a robust capability set for managing Microsoft clients. Unfortunately, the comprehensiveness of SCCM comes at a price, which is a high degree of complexity. SCCM is so complex that only dedicated SCCM experts can hope to operate it to anywhere near its full potential. These experts exist at NETCOM and usually the TNOSC level. At the NOSC level for a garrison, or the BCT level for tactical units, these experts are exceedingly rare. As a result, FA53s and other Army computer specialists are expected to learn to operate SCCM effectively with only a short period of formal instruction and OJT, or no training at all. To make matters worse, operating SCCM is only a small fraction of the daily operations that a NOSC or BCT S6 section is expected to undertake. Additionally, NOSCs and BCTs normally do not have the manning to dedicate even one person to running SCCM. The administration of SCCM tends to be an additional duty for one of the most tech savvy, and usually overburdened, system administrators.

Operating the WSUS was another task performed by NOSCs and BCT S6s, and one that has historically been done well because administering the WSUS is simple and fairly intuitive. AD GPOs are used to ensure that the computers assigned to each OU are allocated to an existing WSUS server. Once assigned to a WSUS server, computers are segmented into deployment groups. If the WSUS is operating in replica mode, it will auto approve and install all updates from its parent WSUS server at Tier 1.[128] In replica mode, the NOSC staff literally does not have to touch the WSUS to patch the computers in its region once an update is approved at Tier 1. If operating in autonomous mode, downloads from the TNOSC Tier 2 WSUS must be manually published. Once completed, update rules can be used to deploy updates automatically to pre-specified collections of clients. The same ease of use claim cannot be made for SCCM. U.S. Army automations officers and signal soldiers working in NOSCs and in BCT G6 shops often report that

[128] Tier 1 for a NOSC is their TNOSC, for a tactical BCT, Tier 1 would normally be Microsoft, or it could be the Division or Corps WSUS if available.

administering SCCM is too complex of a task to be done properly at the NOSC/BCT level, given their current manning levels.[129] As of 2012, the Army provides its new automations officers with 40 hours of training on SCCM. Instructors at the U.S. Army signal center at Fort Gordon estimate that one full-time SCCM administrator is needed per 10,000 nodes.[130] As previously stated, NOSCs and BCTs do not normally have the luxury of a dedicated SCCM administrator.

Another problem with the current IAVM process is the lack of integration between the scanning software and the remediation software. eEye Retina NSS is used to assess current vulnerabilities on the network and a combination of SCCM/WSUS remediates those vulnerabilities. As discussed earlier, this process is far from seamless. Non-Microsoft vulnerabilities, to include third-party updates for numerous devices, and configuration changes, all require the creation of custom update packages, with associated XML detection logic. Even once completed, a difference almost always exists between what Retina says is vulnerable and what SCCM/WSUS reports as vulnerable. Thus, which system to believe? It depends on the organization, but for IA personnel and IAVM compliance inspectors, Retina has the final word. The ability to integrate the network scanner with the remediation mechanism would be a tremendous time saver if effectiveness was not compromised. The delta between Retina NSS and SCCM/WSUS results has led many, including the authors, to distrust the results of retina scans due to many observed "false positives."[131] A further limitation of Retina is that if a computer/network device is offline at the time of a scan, results cannot be obtained. In the authors' experience, this situation has always resulted in machines being missed in the first or second scans, only to surface when all vulnerabilities were supposed to have been completely mitigated, which is one reason why scans done independently by a NOSC and TNOSC almost never agree. Not surprisingly, Army leadership has come to

[129] Personal correspondence with U.S. Army Brigade Automations Officer on March 1, 2012.

[130] Personal correspondence with U.S. Army Signal Center Instructor on March 1, 2012.

[131] A false positive is observed when an information system is verified to be patched for a specific vulnerability, but Retina still reports it as vulnerable. Often, this results from the manner in which Retina verifies the vulnerability is mitigated. Sometimes, the patch or update does not change the signature that Retina uses to determine if a system is vulnerable for a specific IAVM.

favor the reports from SCCM/WSUS over those of Retina.[132] A potential solution could be the integration of the scanning and patching tool, which could potentially remove reporting conflicts between two separate tools.

[132] Personal correspondence with U.S. Army Network Enterprise Technology Command official on February 3, 2012.

IV. ANALYSIS AND OVERVIEW OF CURRENT SOLUTIONS TO THE THIRD-PARTY PATCHING PROBLEM

A. INTRODUCTION

Preceding this chapter, the literature and IAVM process reviews explored past and present cyber threats, with a focus on third-party application vulnerabilities that identified past and current limitations in vulnerability management solutions employed by the U.S. Army. This chapter uses a system engineering approach to determine what requirements an optimal third-party vulnerability management solution would include if it existed. Later in the chapter, currently available COTS patch management solutions are compared to the optimal solution identified by the system engineering approach. A key focus of this chapter is a cost-benefit analysis between the Army's currently identified solution for patch management (SCCM) and readily available COTs solutions. This chapter begins with a brief overview of the system engineering process, and specifically, focuses on how it can assist in identifying the qualities of an ideal third-party patch management solution.

B. THE SYSTEM ENGINEERING PROCESS

1. System Engineering Process Overview

System engineering is defined as "the orderly process of bringing a system into being and the subsequent effective and efficient operation and support of that system throughout its projected life cycle."[133] A system is defined by the Defense Acquisition University as "an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective."[134] System engineering focuses on a top down, integrated, "cradle to grave" approach to the design, development, production, fielding and retirement of a system. The system engineering process begins with the identification of a problem or requirement. The process continues through the design and

[133] Benjamin S. Blanchard, *System Engineering Management*, 4th ed. (New Jersey: John Wiley and Sons, 2008), 1.

[134] Defense Acquisition University, *Systems Engineering Fundamentals* (Fort Belvoir, VA, 2001), http://www.dau.mil/pubs/pdf/SEFGuide%2001-01.pdf, 3.

fielding of a solution that solves the identified problem or requirement.[135] Figure 20 depicts the fundamental steps of the system engineering process.

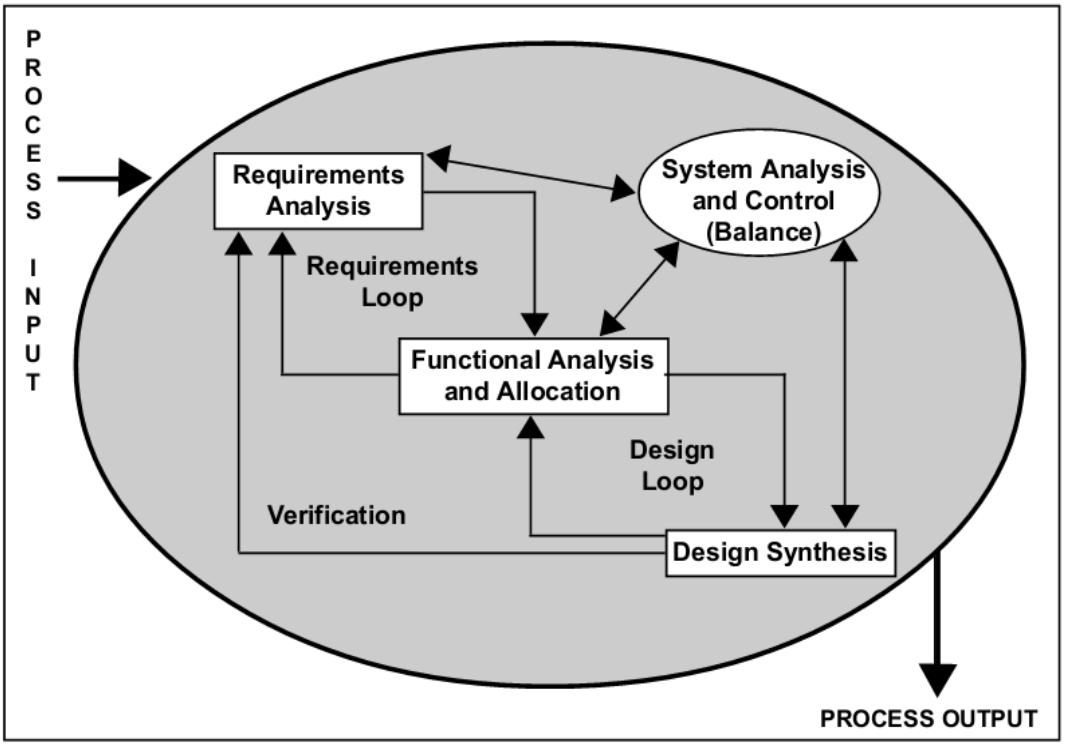


Figure 20. The System Engineering Process[136]

The system engineering process is also iterative. Each phase of the process has the potential to impact previous phases, which requires revalidation. System engineering represents a departure from the way that projects are often run. Normally, a great deal of effort is focused on the design, development and production costs of a system. Unfortunately, the cost associated with system operation and maintenance is often ignored or given insufficient attention. Figure 21 depicts the "iceberg" of systems costs and shows how approximately 75% of the lifecycle costs of a given system are attributed to operations and maintenance.[137] In general, the longer a system is expected to stay in service, the greater the expenditures of back-end costs.

[135] Snyder, "The Department of Defense Must Combat Terrorism with Cyber Attacks," 43.

[136] Defense Acquisition University, *Systems Engineering Fundamentals*, 6.

[137] Blanchard, *System Engineering Management*, 13.

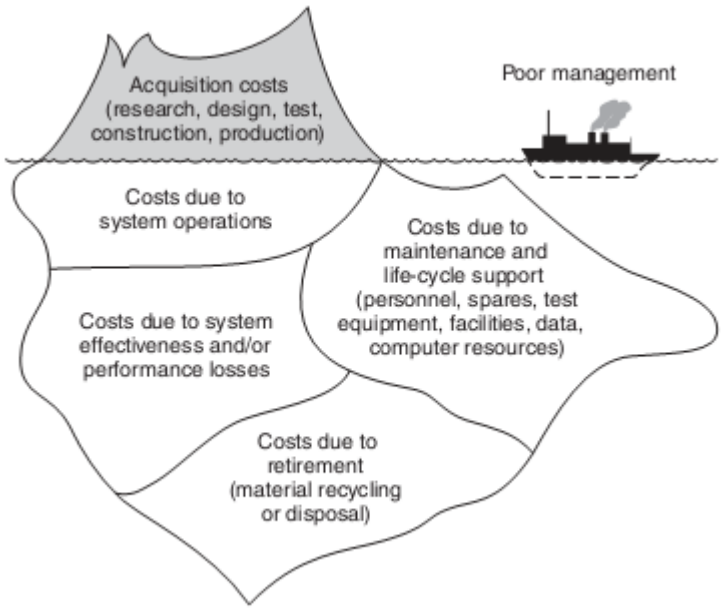


Figure 21. Total System Costs[138]

When multiple systems are combined together, as is the case in a CM system, like SCCM, system engineers refer to this as a system of systems (SoS).[139] A SoS can be thought of as a complex system that is part of a larger hierarchy. Third-party patch management software is by itself a complex software system, which is often combined with another software system that provides operating system vendor patches.[140] The patch management system is often then combined with other complex systems, such as vulnerability scanning software, CM software and many other software systems that are integrated to fulfill a common function, such as device management. Figure 22 depicts a SoS beginning with enterprise NetOps and ending with third-party patch management software (SCUP), which is integrated into the patch management framework of SCCM. Figure 22 is not inclusive of all Army approved NetOps tools.

[138] Blanchard, *System Engineering Management*, 13.

[139] Ibid., 2.

[140] WSUS provides this function for Microsoft operating systems.

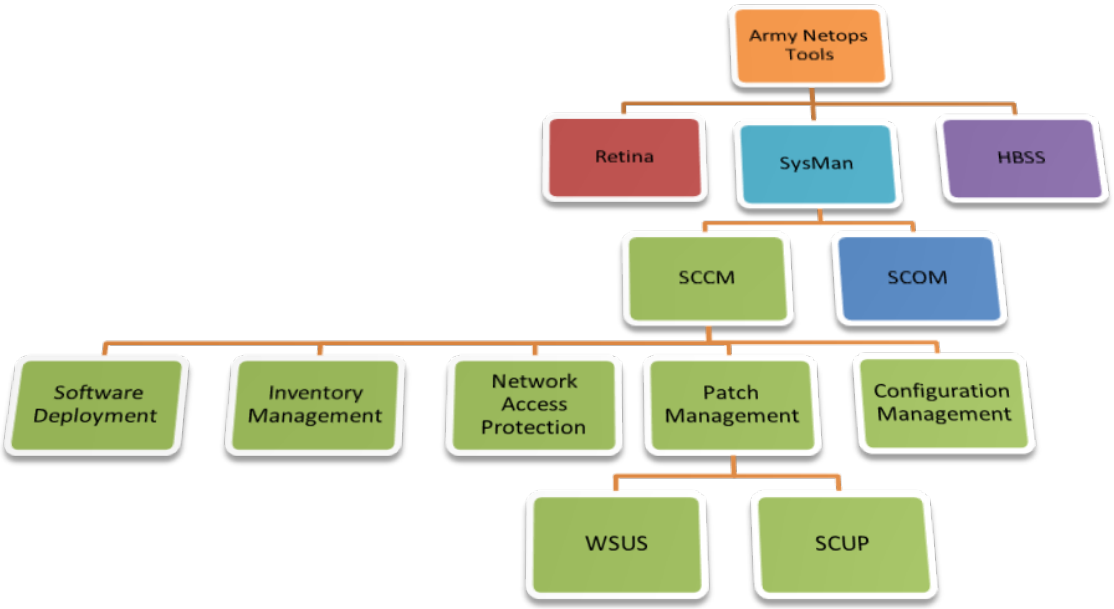


Figure 22. SoS Hierarchy for a Third-Party Patch Management Solution (SCUP) within NetOps

The integration of individual systems into a SoS is a significant concern to system engineers and can be a problem when multiple COTS systems are combined to create a SoS. In the context of a SoS, when each system is integrated to achieve a common goal, each individual system must still meets its original design requirements. In other words, the performance of a system should not be degraded because of integration requirements.[141] A 2011 thesis by MAJ Derek Snyder used the example of an Unmanned Aerial Vehicle (UAV) and a rifle. Both systems combine to form a SoS that fulfills the function of sniper suppression. However, both the UAV and rifle had to be significantly modified to create the SoS.[142] The challenge to the system engineer, when designing the SoS, is to complete this modification without degrading the original performance of the UAV or the rifle, which is not a trivial endeavor.

Aside from the challenges of SoS integration, requirements changes or creep present another significant risk to the system engineering process. Many factors influence

[141] Blanchard, *System Engineering Management*, 207–208.

[142] Derek J. Snyder, "Design Requirements for Weaponizing Man-Portable UAS in Support of Counter-Sniper Operations" (master's thesis, Naval Postgraduate School, 2011).

requirements creep, including lengthy development time, inadequate initial requirements identification, budget constraints and technology changes to name only a few of the top concerns. When this happens, the system in question is usually cancelled, which was the case for the USMC Expeditionary Fight Vehicle (EFV) that was cancelled by Congress in 2011 after nearly 20 years of development and never moved beyond its test phase. The crusader self-propelled artillery system was an Army program cancelled due to requirements shift. This system was meant to replace the Vietnam War era M109 self-propelled howitzer, but was cancelled because of a decision by the Secretary of Defense, Donald Rumsfeld, which essentially said that the Army needed greater strategic mobility. This cancellation meant the end of the crusader, and set out new requirements for wheeled, rather than tracked, fighting vehicles.[143]

To complete the system engineering process, methods from Blanchard and the Defense Acquisition University have been used to create the following seven-step process interconnected by feedback and corrective action loops:

1. Identify and define the problem
2. Systems requirements analysis
3. Functional analysis
4. System design (conceptual, preliminary, detailed)
5. System production and modification
6. System implementation and assessment
7. Retirement

C. APPLICATION OF THE SYSTEM ENGINEERING PROCESS

1. Identify and Define the Problem

The dangers of failing to update operating system, as well as third-party applications, have been well documented in the literature review. The problem for the U.S. Army prior to 2007 was the lack of a standardized enterprise NetOps tool that was both effective and efficient at patching third-party applications. When the Army entered into its first ELA with Microsoft on May 30, 2003, SMS was included in the $78M per-

[143] Warren Vieth, "Rumsfeld, Army Chief at Odds on Weapon System," *Los Angeles Times*, May 17, 2002, http://articles.latimes.com/2002/may/17/nation/na-crusade17.

year licensing fee.[144] It is unclear if the ELA with Microsoft influenced the selection of SMS for enterprise standardization. However, it was not until 2007 that the Army CIO/G6 decided to standardize SMS/SCCM as the Army enterprise tool for configuration/patch management.[145] The close of 2011 saw ARCYBER issue an EXORD mandating the use of SCCM for all Army organizations no later than December 31, 2011; at the time of this writing that mandate is still incomplete[146] Aside from the research and recommendations of the Gartner group made prior to 2007, which aided the Army in selecting SMS/SCCM, a thorough comparison of all available third-party patching applications using a system engineering approach does not appear to have been completed. Assuming that SMS/SCCM was the best option when the Army selected it for enterprise standardization, a great deal has changed since then, which certainly warrants a closer look at alternatives to SCCM. The question still remains, is SCCM the optimal tool to meet the U.S. Army's third-party patching needs?

2. System Requirements Analysis

The purpose of the requirements analysis is to translate customer requirements into functional and performance requirements that define what a system must do and how well it must do it.[147] The objective is to take very general requirements, constrains and enablers, and turn them into system level requirements.

Identification of customer requirements is the first step in the requirements analysis, as shown in Figure 23. System requirements should originate from the customer, who is the person that understands what the system needs to do better than

---

[144] Mark Barnett and Adelia Wardle, "Microsoft Enterprise License Agreement," *Program Executive Office Enterprise Information Systems*, February 11, 2004, http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CC0QFjAB&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2Fc%2F3%2Fe%2Fc3e4206c-931c-4746-a1ed-52f0d19dc5ba%2FWardleBarnette_ArmySymp2004.ppt&ei=4zScT73-FoGliQLK5ux9&usg=AFQjCNHMRmuZf4lk8fMsRm5x-6fOO49q-Q&sig2=65pSNWjyUHnPgMfDGx1JlA.

[145] Ash and Spragg, "NetOps Implementation Update (CMDB, SMS/MOM, SCTS).

[146] Alice Connor, *U.S. Army Cyber Command Execute Order (EXORD) 2011-090 Implementation and Integration of System Center Configuration Management (SCCM) and NIPRNET and SIPRNET*, U.S. Army Cyber Command, Fort Belvoir, VA, September 20, 2011.

[147] Defense Acquisition University, *Systems Engineering Fundamentals*, 32.

anyone else. Essentially, the customer explains the necessary requirements for fixing a problem and the systems engineer devises a technical solution after careful analysis. It is important that the customer is integrated throughout the system engineering processes, provides feedback and refines requirements.

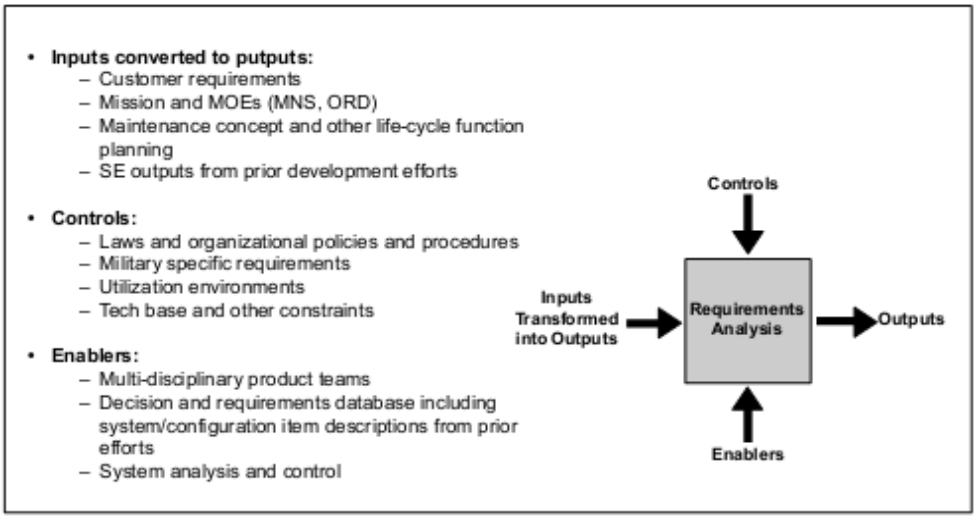


Figure 23. Requirements Analysis Inputs[148]

In this case, the customer is defined as U.S. Army systems administrators at the NETCOM/Corps, TNOSC/Division, NOSC/BCT levels that operate and maintain the enterprise tool(s) used to mitigate vulnerabilities found in third-party applications on U.S. Army information systems. The skill level of system administrators varies widely in the U.S. Army, as it does in corporate America. An effective third-party patch management tool should target the average system administrator and require very little additional training.[149] Customer requirements for a third-party patch management system can be summarized as: securely distribute and install third-party patches to all designated information systems within my area of responsibility with minimal administrator involvement while meeting all IAVM requirements.

[148] Defense Acquisition University, *Systems Engineering Fundamentals*, 37.

[149] Thomas Delaet, Wouter Joosen, and Bart Vanbrabant, "A Survey of System Configuration Tools," Proceedings of the 24th Large Installations Systems Administration (LISA) Conference, *USENIX Association*, San Jose, CA, November 2010, 7.

Customer requirements for patch management were taken from the authors own experience as a NOSC chief, as well as the Army's Common Operating Environment (COE) Architecture and the LandWarNet NetOps Architecture (LNA) for patch management. The basic requirements from the customer's perspective for a third-party patching solution are listed below and include functional, as well as performance requirements:

- System should make the creation, deployment and installation of third-party patches as automated as possible.
    - Must allow for fully automated deployment and installation of approved third-party updates
    - Should be accessible via a web-based interface.
    - Should support both GUI and CLI interfaces.
    - The end user should not be able to cancel the update process.
    - Must allow for update scheduling.
    - Must have built in detection logic to determine what updates are applicable to each information system.
- System must allow for grouping of computers by category.
    - Must allow for grouping clients by operation system, functional designation (e.g., STAMIS, PM, ABCS), equipment class (e.g., server, desktop, printer).
- System must allow for role based permissions.
    - System administrators' permission level must be limited to their group's assigned role within the hierarchy.
- Third-party patches should be created at the top and disseminated down the hierarchy.
    - Third-party patch packages should originate at the top level (Tier 0) and allow inheritance and approval by child servers.
    - Each level of the hierarchy must retain the ability to create custom third-party patches to meet organization specific requirements.
- System should be the same at every organization in the Army.
    - All organizations in the Army, including tactical units, should be using the same tool.

- System should be scalable to the DoD level.
    - Must be scalable to support at least one million Army information systems with a single hierarchy.
    - Should be scalable to support up to 10 million DoD information systems with a single hierarchy.
    - Must allow for child sites to choose what updates to approve for deployment from parent server or allow for replication of parent server patch content and approvals.
    - Should be scalable to a minimum of four tiers, to include DoD level, Army level (NETCOM), TNOSC Level and NOSC level.
    - Must be scalable to a minimum of three tiers (NETCOM, TNOSC, NOSC).
- System should require minimal training for basic operation.
    - Should require no more than eight hours of formal training combined with three days of OJT to attain basic operator level proficiency.
    - Must include detailed online help and documentation.
    - Should include a basic “10-minute” tutorial.
- System should be simple to field and configure.
    - Should be a COTS or open source software solution.
    - Must not require a special team from the CIO/G6 or NETCOM level to field.
    - Fielding should be possible by organic TNOSC/NOSC personnel by following fielding documentation provided by NETCOM.
    - Should make use of existing virtualization technology and not require the purchase of additional physical servers.
    - Organic TNOSC/NOSC system administrators must be able to fully configure the newly installed system using supplied documentation.
    - Should be available for download on a CAC authenticated LWN portal.
    - Must make use of existing Army IT infrastructure.

- System should be reliable and effective.
    - Must maintain a reliability measure of no less than 99.9% uptime.
    - Must have a first pass patch installation success rate of no less than 95% for correctly configured clients.
    - Future support must be planned for the tool by the vendor for at least five years.
- System should patch as many platforms as possible, but primarily Windows-based information systems.
    - Must support all Windows-based clients.
    - Should support Linux, Unix and Macintosh-based clients.
    - Should support networking devices.[150]
    - Should support mobile devices (Blackberry, Android, iOS)
- System must be accredited for operation on the GIG and LWN.
    - Must meet Certificate of Networthiness (CON) requirements.
    - Must achieve FIPS 140-2 and Common Criteria Evaluation and Validation Scheme (CCEVS) validations.
    - Must make use of PKI to validate authenticity of updates.
- System must provide compliance reporting for all assets.
    - Must maintain a database of all assets.
    - Must provide compliance reports by vulnerability for all assets and by individual IS up to Tier 0 level.
    - Tier 0 system must have full reporting visibility of all child server assets.
- System should interface with Retina NSS or Enterprise network scanning solution.
    - Should take results directly from Retina NSS scans for remediation.
    - Results from Retina NSS and system should match.
- System must support remote sites.
    - Must be capable of updates over WAN links as slow as 56 Kbps.
    - Updates must be made available as soon as a client comes online.

[150] Cisco, Foundry, Netgear and other devices, including routers, switches, firewalls, IDSs, IPSs,

In addition to customer requirements, existing and projected constraints need to be considered. Constraints limit the feasible options to the system engineer. Constraints can be internal or external to the Army. Internal constraints consist of Army regulations and policy that must be followed. External constraints often take the form of federal or DoD directives to which the Army must also adhere to.[151] Key constraints impacting the design of a third-party patching solution are taken from the LNA, COE, the author's personal experience and Army/DoD regulations and are listed below.

- Declining DoD and Army budgets.
    - System should represent a favorable ROI in comparison to alternatives.
- Political considerations, including biases.
    - Current leadership may have biases favoring SCCM.
    - U.S. Army already has an ELA with Microsoft.
    - U.S. Army has invested very heavily in the current SCCM 2007 infrastructure.
- Technical expertise of system administrators at each level.
    - Technical expertise and manning levels generally decrease from the NETCOM to NOSC levels.
- Army Regulations.
    - AR 25-2 Information Assurance does not mandate any specific type of patch management solution; it only specifies IAVM process requirements.
    - AR 25-1 and AR 25-2 require that all information systems generate audit logs and limit logon attempts to three before denying access to a specific account.[152]
- U.S. Army Mandates.
    - Common Operating Environment (COE) Implementation Plan, NOV 2011.
    - COE Architecture, OCT 2010.

[151] Defense Acquisition University, *Systems Engineering Fundamentals*, 37.

[152] Headquarters, Department of the Army, *AR 25-2, Information Assurance*, 23.

    - Army Golden Master (AGM) Operating System usage mandatory for desktop/server environment.
    - Army CIO/G6 moratorium on fielding of NetOps tools to BCTs.
- Federal/DoD Regulations.
    - FIPS 140-2 compliance mandate.
    - Federal Desktop Core Configuration (FDCC).
    - Common Criteria Evaluation and Validation Scheme (CCEVS).
    - DoDi 8410.02 NetOps for the Global Information Grid (GIG).
    - DoD Directive 8500.01E Information Assurance.
    - DoD 2011 Strategy for Operating in Cyberspace.

Once requirements and constraints are identified, it is necessary to consider enablers in the organization that aid in the creation of the new system. The enablers for the third-party patching system are as follows.

- Cyberspace is now recognized as an operational domain, equal to land, sea, air and space, by the DoD and U.S. Army.[153]
- DoD Cyber organizations (CYBERCOM).
- U.S. Army Cyber organizations (ARCYBER, NETCOM, CIO/G-6, TNOSC, NOSC).
- Assistant Secretary of the Army Acquisitions, Logistics and Technology (ASA/ALT).
- Army relationships with service providers, especially Microsoft and Dell.
- Institutionalized experience with vulnerability mitigation within the IA community.

The key impact of constraints on the customer requirements for the third-party patching system is that the system must be deployed on either physical or virtual servers running AGM Microsoft Server 2008 or newer. In other words, it must meet FIPS 140-2 compliance, CCVES validation and CON validation. In addition, due to budget considerations, it must have favorable lifecycle costs in comparison to its competitors. The next step in the process is to conduct a functional analysis.

[153] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace."

3. Functional Analysis

The purpose of a functional analysis is to provide a description of a system in terms of what it does logically, and what level of performance it is required to achieve while meeting its logical functions, which is accomplished by decomposing higher level functions, identified in the requirements analysis, into lower level functions.[154] Functions are defined as an operation a system must perform to meet its stated objective(s).[155] The functional analysis also identifies the specific resources required at the subsystem level and below. It is an iterative process of decomposing requirements from the system level to the subsystem(s) level, with the objective of identifying input design criteria and constraints that impact system development.[156]

The functional analysis normally begins with problem identification and needs analysis. The first step is to identify all functions that the system must perform to fulfill the needs of the customer. One of the primary tools used to complete a functional analysis is the functional flow block diagram, which is utilized to structure system requirements into functional terms. Upon completion, engineers identify design functions, test operational functions, production functions, maintenance functions and retirement/disposal functions as required. Each function is then evaluated to ensure that input-output requirements, constraints and resources required are satisfied.[157] Figure 24 shows each of the elements that should be identified to conduct a functional analysis.

[154] Defense Acquisition University, *Systems Engineering Fundamentals*, 32.

[155] Blanchard, *System Engineering Management*, 71.

[156] Ibid., 72–73.

[157] Ibid., 71.

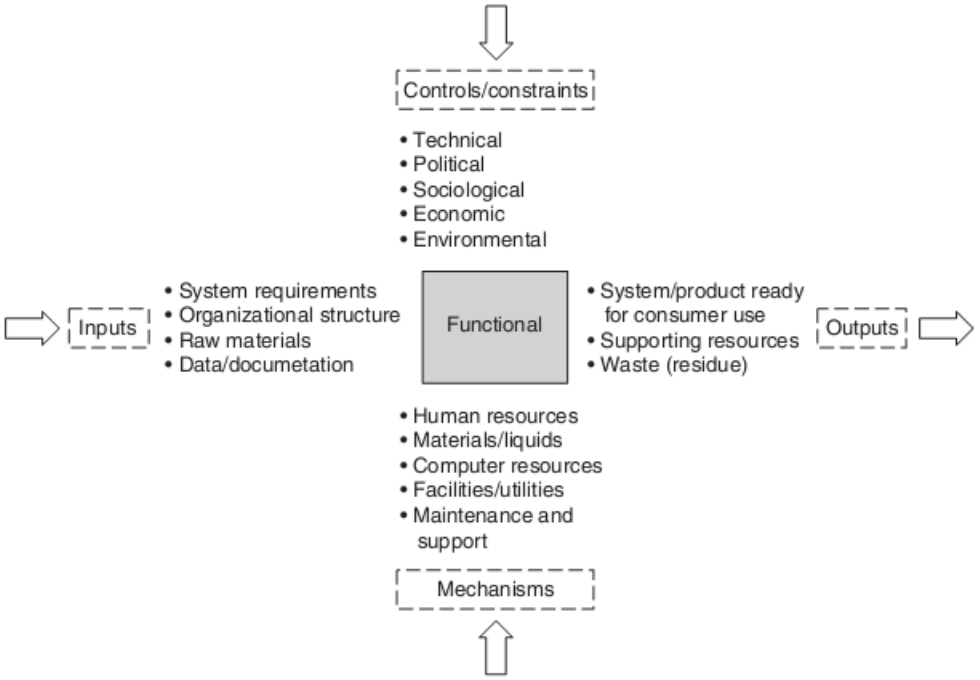


Figure 24. Functional Analysis Template Used to Identify Resource Requirements[158]

One of the key requirements of the functional analysis is to trace high-level system requirements to detailed design requirements to ensure that each high-level requirement is addressed in the system design. This requirement also allows for justification of specific system design choices by making it possible to start at a low-level and proceed up the functional flow block diagram to the high-level customer requirement.

In evaluating functional requirements, COTS solutions should be considered as a viable alternative to in-house development. Figure 25 depicts how a COTS system could be identified through a functional analysis and trade-off studies.

[158] Blanchard, *System Engineering Management*, 83.

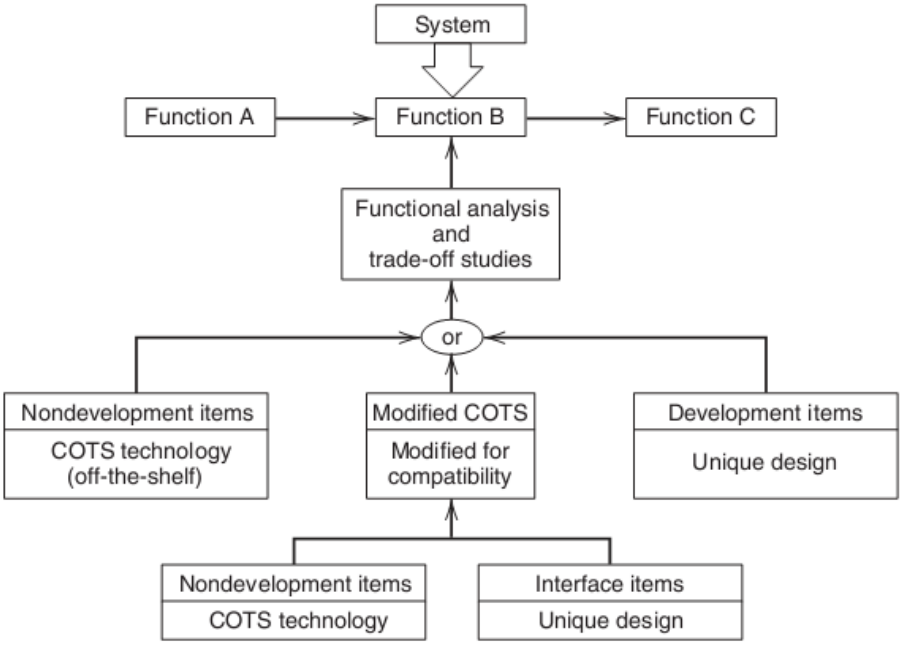


Figure 25. Identification of COTS Systems using a Functional Analysis[159]

It is important to evaluate each COTS system to determine functional shortfalls that must be addressed to meet customer requirements, which may necessitate contacting the software supplier with a request to modify a certain product. Given the size of the DoD and the relationship it has with industry, it is certainly possible for functional improvements/modifications to be made to many COTS systems. Selection of COTS systems is preferred due to the ability to field existing, thoroughly tested systems rapidly. Additionally, COTS systems generally result in significant cost savings and leverage software development expertise that does not exist or is in extremely limited supply in the DoD.[160] The next section uses the requirements analysis to describe what an optimal third-party patching solution looks like for the U.S. Army.

[159] Blanchard, *System Engineering Management*, 83.

[160] Ibid., 81.

D. OVERVIEW OF EXISTING PATCH MANAGEMENT TECHNOLOGY

1. Introduction

The purpose of employing a configuration or patch management solution is to automate routine functions performed on client devices. The most significant of these functions includes software deployment, asset inventory, and patch deployment. Very few patch management solutions are limited to only deploying third-party patches. Typically, patch management software addresses operating system patches, as well as third-party patches. The trend over the last decade has been to "operationalize" patch management solutions by combining them with other systems that perform a complete suite of device management capabilities.[161] Systems in this category include Microsoft SCCM, Symantec Altiris, Avocent LANDesk, IBM Tivoli, CA Client Automation, Dell KACE and others. Other systems focus mostly on patch management, but also offer some CM capabilities, which includes offerings like Microsoft WSUS, SolarWinds Patch Manager, Lumension Endpoint Management and Security Suite, VMware Vcenter Protect Essentials Plus, ScriptLogic Patch Authority Ultimate and many others. The choice of selecting a patch management tool should be driven by customer requirements.

2. Point vs. Client Management Tools

The distinction between dedicated patch management solutions, which can be considered point products, and client management solutions continues to blur. Point products historically have offered patch management capabilities only. They primarily filled in the patching gap left by Microsoft WSUS for organizations that primarily ran Windows. Today, point solutions tend to be much more full featured, with the ability to do asset discovery, vulnerability detection, report generation, CM, license management, network performance management, software package deployment, and power management. In general, point products tend to excel at patch deployment in relation to their other capabilities. Microsoft WSUS is the perfect example of a patch management point system that performs its rather limited purpose very well.

---

[161] Mary Brandel, "How to Compare Patch Management Software," *CSO Online*, 2009, http://www.csoonline.com/article/507070/how-to-compare-patch-management-software?page=4.

Client management tool development began with Microsoft SMS in 1994 and has expanded to include 14 major competitors as reported by Gartner in its annual Magic Quadrant for Client Management Tools report.[162] These tools are intended to manage all aspects of a client's lifecycle, ranging from operating system or image deployment, to client retirement and everything in-between. At their core, client management tools focus on CM and tend to have patch management capabilities modularly included, which was the case with SMS that lacked any patching capability, beyond the ability to execute scripts. By 2007, SMS had morphed into SCCM, which incorporated WSUS to handle Microsoft updates. SCCM 2007 allowed for the use of the newly created SCUP tool for authorizing third-party patches and software packages, but only as an add-on module.

Recent capability additions to client management tools include performing administrative tasks on virtual clients, virtual applications, mobile devices and Mac operating systems.[163] Since its introduction in 2007, SCCM has dominated the CM market. The Gartner group identified SCCM as the segment leader in both its 2009 and 2012 Magic Quadrant reports, which represents a significant improvement over SMS. Estimates by BDNA put SCCM at managing 100 million desktops devices globally, which equates to about 50% of the business market.[164] Gartner attributes much of the success of SCCM to "Microsoft's licensing strategy of including it in the core and enterprise client access license bundles." It also notes that many organizations have switched to SCCM if they have an ELA with Microsoft to save money on licensing costs.[165]

3. Agent vs. Agentless Client Management Tools

One choice that needs to be made when selecting a patch management or client management solution is to decide whether to use an agent-based or agentless solution.

---

[162] Terrence Cosgrove, *Magic Quadrant for Client Management Tools*, Gartner Inc., January 31, 2012.

[163] Ibid.

[164] Martin Thompson, "Microsoft SCCM (ConfigMgr) Plug-is Group Test," *The ITAM Review*, February 2012, http://www.itassetmanagement.net/microsoft-configmgr-plugins/.

[165] Terrence Cosgrove, *Magic Quadrant for PC Configuration Life Cycle Management Tools*, Gartner Inc., November 24, 2009, 10.

Agentless systems use push technology whereby a server scans each device on the network and reports back to a central server that takes action based on scan results. These systems have several advantages over agent-based systems. One advantage is ease of deployment, which is a result of clients not requiring an agent to allow for the rapid management of large networks. Another advantage is the ability to at least detect clients that do not have an agent. Some clients on the network may not be supported by an agent; the agentless system will at least make their existence known if they cannot be managed. An additional benefit of an agentless system is that it requires less management effort because system administrators do not have to worry about agent deployment to clients. A major disadvantage of agentless systems is that they do not work well for clients that reside in a DMZ, roaming/inactive clients, or in networks with limited bandwidth. Agentless systems are also not as effective at asset inventory, as a scan must be completed to obtain an inventory.[166]

Agent-based systems, such as WSUS and SCCM, offer several benefits over agentless systems. One of the largest advantages is that agent-based solutions have a wider range of management control over a device and much better asset inventory control. Part of the reason for this advantage is that the client's agent checks in with the management server at predefined intervals; or in other words, inventories can be kept current without additional action on the part of a system administrator. Agent-based systems also function more effectively on clients with limited bandwidth and roaming clients because they do not depend on the management server reaching them; they report to the server when they come online and then receive any actions the server's policy dictates.[167] The primary disadvantage of an agent-based system is that deploying agents to all clients is time consuming and can be problematic, which can be alleviated somewhat by using an AD group policy to instruct clients to download and install an agent upon authenticating with their DC. Another disadvantage of agent-based tools is that a one-one relationship exists between agent and operating system. In other words, unique agents must be supported by the tool. Some tools, such as SCCM, circumvent this

[166] Brandel, "How to Compare Patch Management Software."

[167] Ibid.

situation by utilizing add-ons like Quest Management Xtensions (QMX). Management of non-Microsoft clients is becoming an increasing concern as more Macs and mobile devices make their way onto Army networks. Currently, the Army only allows Research in Motion (RIM) Blackberry smartphones on the LWN. AR 25-2 states, "Employee owned Personal Electronic Devices are prohibited for use in official communications or connections to Army networks."[168] The high demand for Android and iOS devices among soldiers will likely result in the iPhone, iPad and Android devices making their way onto the LWN in the near future. The DoD recently authorized the use of the Android based Dell Streak 5 on the GIG, so it is likely that other Android devices are not far behind.[169]

E. FINDINGS DERIVED FROM THE REQUIREMENTS ANALYSIS

1. Introduction

The purpose of this section is to determine what characteristics an optimal third-party patching solution for the U.S. Army should have, which is accomplished by further analyzing the findings of the requirements analysis with the fundamentals presented in the functional analysis section. The ideal third-party patching solution should support seven elements.

2. Scalability and Architecture

Two main architectural factors impact scalability. The first is the number of clients that each individual server in a particular deployment can support. For most vendors, the number is less than 20,000 clients per server. The second factor is the number of clients that a single hierarchy can support. Most tools fall into one of three categories. In category "A," tools lack hierarchy support. In this model, clients connect to a single master server, and scalability is limited by the number of clients the master server can support. Category "B" tools support a hierarchy of servers, in which a master server maintains direct control of child servers, and as a result, all clients in the hierarchy.

---

[168] Headquarters, Department of the Army, *AR 25-2, Information Assurance*, 46.

[169] Elizabeth Montalbano, "DOD Approves Dell Android Tablet for Use," *InformationWeek Government*, October 31, 2011, http://www.informationweek.com/news/government/mobile/231901988.

This model has limits to scalability as child servers are added to the hierarchy. Eventually, the master server becomes overloaded because it must maintain a complete data set about every client in the hierarchy. Products like Microsoft SCCM fall into this category, as do most CM tools. Category "C" tools implement a server hierarchy in which the master server does not maintain command and control of all child servers and their assets. It maintains visibility of the assets managed by child servers by including a roll up of data one-tier down. Thus, a master server operating at Tier 0 collects data summaries from each of its child servers at Tier 1 only. Tier 1 child servers collect data rollups from Tier 2 child servers and so on. This solution is the most scalable of the three possibilities discussed and can easily accommodate scalability to the DoD level. Microsoft uses this model to manage millions of computers with its windows update service, which is essentially a public version of WSUS.[170]

To support the U.S. Army's current client environment, along with anticipated growth, the optimal tool should support at least one-million client devices using a single, multi-tiered, deployment architecture. If multiple hierarchies are used in a deployment, nearly any tool can achieve unlimited capacity, but at the cost of greatly increased management effort. Given the emphasis within the DoD on interoperability, the tool should also be scalable to support the entire seven-million information systems currently in use with the DoD, with a single hierarchy, which can safely be assumed will continue to expand.[171] Third-party patch content and policy should be centralized and created at the top tier. Downstream servers located at each TNOSC and NOSCs should have the ability to replicate the settings of an upstream server, or operate autonomously, by using the upstream server as a data source only that allows for a degree of flexibility necessary to accommodate disparate computing environments. An example is the need for NOSCs operating in Korea, Okinawa, Japan and other regions to install language specific software updates. This level of flexibility would be mandatory if the tool were to be used at the DoD level, in which each service would require a high degree of autonomy from a

[170] Personal Correspondence with Defense Information Systems Agency (DISA) official on April 10, 2012.

[171] Department of Defense, "Department of Defense Strategy for Operating in Cyberspace."

DoD root server. Thus, the optimal tool should be able to support a four-tiered deployment architecture to accommodate adoption by the DoD. This architecture is depicted in Figure 26, which also shows how any client can be associated with any authorized upstream tool, which accommodates organizations that operate without the support of a NOSC or TNOSC. The ability of an existing tool to support a tiered architecture with one to 10 million clients will eliminate many current solutions that cannot scale to this level.

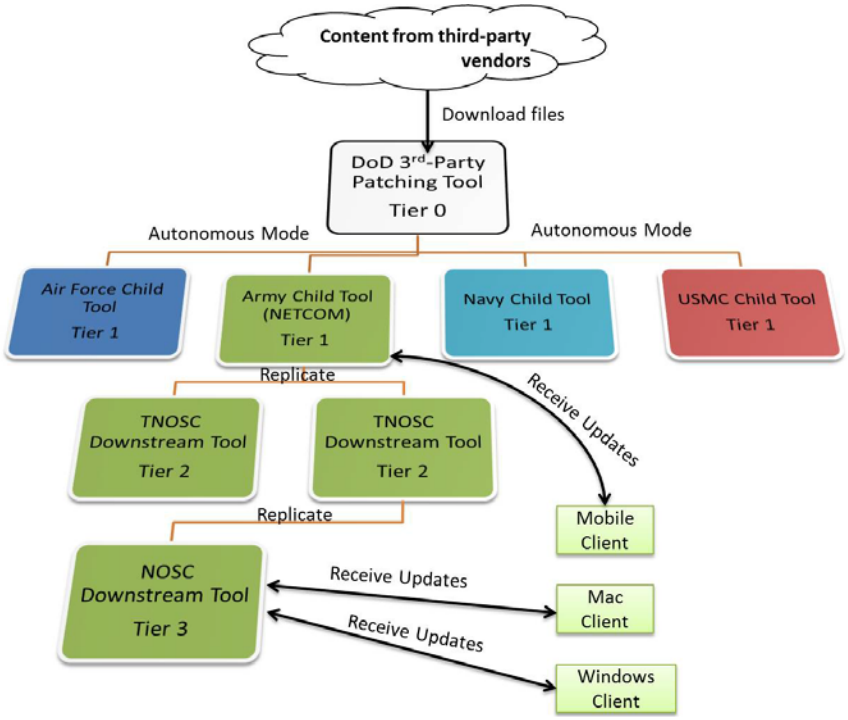


Figure 26. Proposed Optimal Tool Architecture

3. Ease of Deployment and Use

One of the key requirements of the optimal tool is ease of use. The average system administrator at the NOSC level or higher should be capable of deploying this tool onto existing hardware and configuring it with supplied documentation. Documentation should be highly detailed to support troubleshooting efforts. The tool should also include a 10-minute tutorial video, which provides a good means of quickly

introducing the basic functions and operation of the tool to new system administrators. The tool should require no more than eight hours of formal training, combined with three days of OJT for a new system administrator to reach basic competence that includes the ability to create client collections and custom patch content, approve updates from an upstream server, authorize deployment(s) of updates, run compliance reports and conduct basic troubleshooting. This tool's interface should be GUI based to support the average system administrator, but should also retain a CLI to support more advanced system administrators. A standard web browser should be the primary means to control the tool.

To support ease of deployment, the tool should operate on current VMware ESX virtual servers deployed in data centers across the Army, which greatly diminishes the need to procure additional servers to support fielding. In addition, the tool should be made available for CAC authenticated download on a LWN portal, such as AKO or CHESS. The tool should also be hosted on the standard AGM server operating system, which is currently Microsoft Server 2008 R2 and also utilize Microsoft SQL Server 2008 R2 or the newest authorized version as its database server.

4. Functional Capability

The primary function of the tool is to deploy third-party patches to clients residing on the LWN. The tool should accomplish this function by automating the deployment of patches to the maximum extent possible that should be achieved by using an agent, pull-based system to reduce the number of steps necessary for the system administrator to deploy updates and increase the probability of success. If the tool is in replica mode, the administrator only needs to have client collections identified to receive updates. The tool then automatically deploys updates based on its policy settings. If the tool is operating in autonomous mode, the administrator manually approves each update, which authorizes the tool to push patches to previously created client collections.

The optimal tool should also have built-in detection logic, which allows it to take client data from each agent and compare it to a database that contains information on the desired stare of each client. In this way the tool will know when a client is out of compliance and initiate the update process. Clients that are not up to date should be

quarantined from contact with other devices, with the exception of update server(s) until remediation is completed. This capability should be exercised at the discretion of local TNOSCs or NOSCs. To help ensure that all clients have an agent installed, the tool should interface with Microsoft AD to provide awareness of all clients on the domain. Deployment of the agent to clients should be done primarily by AD group policy, which helps to ensure that all clients on the domain have the client installed. The tool should also have the capability to repair any agents on malfunctioning clients.

Being the tool is pull based, clients will check-in with update servers that scan them for any missing patches and remediate if necessary. Client check-in time should be configurable in gradients of one-minute intervals. The update process should inform the end user that the update process is occurring, but not allow the user to cancel the process. The tool should allow the user to delay the update for no more than 10 minutes. If the user attempts to avoid the update process by rebooting, the client's agents should initiate the update process immediately without user consent. To ensure the authenticity of communication between a client's agent and the tool, certificate-based encrypted authentication must be used.

The tool should have the capability to group clients by device type, operating system and functional designation. The tool should also allow for update scheduling, which improves performance in bandwidth constrained environments. Administrative control of the tool should be hierarchical, with access levels based on security group membership, which is very similar to the system utilized in Microsoft AD.

The tool should be able to patch a wide range of clients. Ideally, the tool should be able to patch any potential clients authorized access to the LWN, including Linux, Unix, Mac, Android, iOS, BlackBerry and networking devices. In other words, the tool would have to support numerous disparate agents, and/or utilize an agentless push mechanism. Use of client agents is desirable due to their superior functional capability and their ability to deal effectively with remote clients in comparison to agentless systems.

The tool should be capable of generating automated compliance reports that allow visibility of all Army clients from a single web-based interface. These reports should provide granularity down to the individual client, as well as client rollups at the organizational, regional, theatre, Army and DoD level. The data from these reports must be made available to other sub-systems in the SoS to allow for complete asset visibility.

Integration with the Retina NSS is another capability the tool should possess so that Retina NSS vulnerability scan results match those generated by the tool, or Retina NSS is the scanning agent for the tool. If care was taken to ensure that each update package utilized the same detection logic as Retina NSS, the inconsistencies between the two tools could be eliminated or greatly reduced.

5. Interoperability

Although this tool is specified for U.S. Army use, the tool should have the characteristics that allow it to be adopted as a DoD-enterprise solution without modification. The key criteria to support DoD requirements is scalability to 10-million clients and integrated reporting on the third-party patching levels of all clients. If implemented as a DoD level solution, a master server operated by CYBERCOM should be capable to providing third-party update packages to child servers operated by each service, as shown earlier in Figure 26.

Like the Army, the client environment in the majority of the DoD is Windows based and often operates in a distributed manner. The Navy and USMC in particular often operate in extremely disjointed and bandwidth constrained environments. The tool should have the ability to operate on small-footprint virtualized servers, while offering control of bandwidth used by the update process.

To support interoperability within the Army, the tool should be standardized under GNEC 6+1 as an approved NetOps tool to allow NETCOM to mandate its usage by all organizations in the U.S. Army.

6. Regulatory Guidance

To achieve operation on the LWN, the tool must be capable of meeting Army and DoD regulations and mandates. The tool must be capable of meeting FIPS 140-2 and CCEVS validation to operate on the GIG. To operate on the LWN, the tool must also meet CON requirements, which include FIPS 140-2 and CCEVS, but also serve as a final check by the U.S. Army to ensure the software supports the Army's goals of standardization, supportability, sustainability, interoperability and compliance with federal, DoD and Army regulations and mandates. In addition, the tool must meet requirements in AR 25-2 that mandate logon attempts and user logon data must be stored.[172]

7. Reliability and Performance

Since the tool operates continuously on the network and provides updates to clients, it should achieve as close to 100% reliability as possible. It is reasonable to expect the tool to achieve 99.9% uptime, with concessions made for occasionally rebooting the virtual server it resides on due to planned maintenance, such as patch deployment or software upgrades. The tool should also be capable of achieving a 95% or greater first pass patch deployment and installation success rate on clients with a properly functioning agent. The tool should also be responsive, which means that the web interface used to control the tool should load within five seconds given 100 Mbps or better LAN connectively. The tools responsiveness should not degrade by more than 20% as it reaches the upper limit of its client capacity. The tool should also respond quickly to user inputs once the interface loads. Response time should average no more than two seconds from command issuance by the system administrator to execution by the tool. In addition, the vendor of the tool should plan to support continued development tool development for at least five years.

[172] Headquarters, Department of the Army, *AR 25-2, Information Assurance*, 23.

8. Cost

The cost of the tool should be competitive with market leaders. In accordance with the COE, open source tools should be given primary consideration, followed by COTS tools, GOTS tools, with in-house development as a last resort, which serves to reduce cost and expedite fielding. Ideally, the optimal solution should cost less on a per-client basis, by taking into account lifecycle considerations, in comparison to the current solution. The next section provides an overview of existing COTS patching solutions.

F. ANALYSIS OF ALTERNATIVES

1. Overview of Alternative Tools

This comparison considers four types of contenders. As mentioned earlier in the chapter, these tools all have much greater functionality than just deploying third-party patches. Only the tool attributes that contribute in some way to the function or use of the third-party patching tool, as identified in the requirements analysis and the findings derived from the requirements analysis, are used as a basis for comparison.

The first tool to be considered is the Army's current solution, Microsoft SCCM. Microsoft made several significant improvements to SCCM 2012, which is a release candidate at the time of this writing. NETCOM has already indicated that it will be upgrading SCCM 2007 to SCCM 2012 as soon as testing is complete.[173] The second type of solution considered is SCCM's top competitors, which were identified as segment "leaders" by Gartner's 2012 Magic Quadrant for Client Management Tools report.[174] All tools in this category, including SCCM, are full featured CM suites that include at a minimum: OS deployment, inventory, software distribution and patch management. Most also include support application virtualization, MDM, power management, software packaging, security CM, remote control and software usage monitoring.[175] The third type of contender considered is the top open source CM solution, which is CFEngine 3. The

[173] Susan Monahan, "GNE SysMan Updates," Proceedings from the LandWarNet Conference, *Armed Forces Communications and Electronics Organization*, Tampa, FL, April 23, 2011.

[174] Cosgrove, *Magic Quadrant for Client Management Tools*.

[175] Ibid.

final type of solution considered is WSUS-extension tools. These tools are identified in Table 1, which also shows the tool category and type.

VENDOR	TOOL	TOOL CATEGORY	TOOL TYPE
Microsoft	System Center Configuration Manager (SCCM) 2012	Current Solution	Client Management Tool
Symantec	Client Management Suites (Altiris)	Top Competitor	Client Management Tool
LANDesk	LANDest Management Suite (LDMS)	Top Competitor	Client Management Tool
IBM	Tivoli Endpoint Manager (TEM)	Top Competitor	Client Management Tool
HP	Client Automation (HCPA)	Top Competitor	Client Management Tool
Open Source	CFEngine 3	Top Open Source Competitor	Client Management Tool
SolarWinds	Patch Manager (PM)	WSUS Extension	Point Tool
eEye Digital Security	Retina CS	WSUS Extension	Point Tool
Open Source	Local Update Publisher (LUP)	WSUS Extension	Point Tool

Table 1. Contenders Listed by Category and Type

2. Microsoft System Center Configuration Manager 2012 (SCCM 2012)

SCCM is by far most popular and widely used client management tool commercially. It is a full featured CM suite that targets large organizations that are primarily Windows based. SCCM 2012 represents a major improvement over the 2007 version, which Gartner mentioned it never considered a "best of breed" tool. Major changes to SCCM 2012 include the introduction of role-based access controls, internal sites and hierarchy improvements, a shift to user centric management, a new console, improvements to software updates, including automatic approvals (which were not available in SCCM 2007) and deployment and integration with SCUP. SCCM integrates with AD for client discovery and uses its own agent in addition to the Windows Update Agents (WUA).[176] SCCM 2012 does not offer an agent for non-Microsoft clients. It uses Exchange ActiveSync to allow for limited MDM for mobile devices connected to

[176] Meged Ezzat, "What's New in Configuration Manager 2012 "SCCM 2012"—Part 1—"Overview," *Microsoft TechNet,* August 10, 2011, http://blogs.technet.com/b/meamcs/archive/2011/08/10/what-s-new-in-configuration-manager-2012-sccm-2012.aspx.

enterprise Exchange servers. Overall, SCCM is a mature product with outstanding third-party support due to its popularity, which allows for add-ons like QMX, to help compensate for its lack of OS support for Mac, Linux and Unix out of the box. Even though SCCM is built on the WSUS framework, it is not as scalable as WSUS because the top tier SCCM server in the hierarchy takes control of every server below it in the hierarchy. In other words, all the data, not just rollup data, must be replicated to the master SCCM server. The upper capacity for a single hierarchy in SCCM 2012 is 400,000 clients;[177] thus, deployment to support the LWN would require at least two separate hierarchies. Scaling the solution to the DoD level would require over 20 hierarchies, and while technically possible, is not feasible. One significant drawback of SCCM is its complexity. It requires a high level of knowledge to deploy and use successfully.[178] It cannot be setup and put into operation by a typical system administrator at the NOSC level. Another weakness of SCCM 2012 continues to be the use of SCUP, which currently only offers third-party patches from three vendors including Adobe, HP and Dell.[179] A consideration when migrating from SCCM 2007 to 2012 is that the new version of SCCM operates natively in 64-bit mode, which is good for performance, but it also prevents an in-place upgrade. A new SCCM 2012 environment must be stood up alongside the existing 2007 deployment, which is a very difficult task.[180]

3. Symantec Client Management Suites (Altiris)

Symantec acquired Altiris in 2007, combined it with several in-house tools, and rebranded it as Client Management Suites (CMS). Using CMS requires the installation of Symantec management platform, which provides the foundation for CMS and allows the use of other Symantec products, such as Server Management Suites. CMS is a popular

---

[177] Microsoft, "Supported Configurations for Configuration Manager," *Microsoft TechNet*, 2012, http://technet.microsoft.com/en-us/library/gg682077.aspx#BKMK_SupConfigSystemReqs.

[178] Cosgrove, *Magic Quadrant for Client Management Tools*.

[179] Microsoft, "Third-Party Custom Catalogs for Configuration Manager 2007 and System Center Essentials 2007."

[180] Paul Schnackenburg, "Microsoft System Center: The New Look of SCCM," *Microsoft TechNet Magazine*, March 2011, http://technet.microsoft.com/en-us/magazine/gg675930.aspx.

CM tool with a large installed base and support community.[181] Mobile devices are not natively supported by CMS, but Symantec offers this capability with its mobile management add-on.[182] Support for patching Microsoft, Mac, Linux and Unix OS's and third-party applications is provided by the Altiris patch management solution, which is integrated with CMS using either a Windows, Mac or Linux agent. Each client agent communicates with a Notification Server (NS) that collects configuration information and sends it to a SQL database. The NS then determines what updates need to be applied. Updates can be automatically applied to client groups, or manually deployed. CMS supports a standard hierarchy, which allows for tiered deployment of NSs. Child NSs can inherit all or part of parent NS permissions that permits replication of parent NS, or operation autonomously.[183] While CMS is a very comprehensive CM solution, it is complex and difficult to deploy and administer. Gartner reported that CMS has had a number of stability and scalability problems. In addition, many CMS customers are concerned about Symantec's dedication to Altiris products.[184] CMS is scalable to support the needs of a large enterprise, but not one as large as the U.S. Army or the DoD. Each NS can support up to 10,000 clients. The upper limit of a single CMS hierarchy is approximately 100,000 clients.[185]

4. LANDesk Management Suite 9 (LDMS)

LDMS 9 is one of the most functionally complete CM tools available. It is a modular suite comprised of the LANDesk inventory manager, power manager, system manager and server manager. LDMS architecture is relatively simple. Clients

---

[181] Paul Schnackenburg, "Microsoft System Center: The New Look of SCCM."

[182] Symantec, "Altiris Client Management Suite 7.1 from Symantec," 2011, http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-client_management_suite_7_1_DS_21178300.en-us.pdf.

[183] Symantec, "Altiris Patch Management Solution for Windows 7.1 from Symantec User Guide," 2011, http://www.symantec.com/business/support/resources/sites/BUSINESS/content/live/DOCUMENTATION/3000/DOC3505/en_US/PatchWindows_user_guide.pdf. 2011.

[184] Ibid.

[185] Symantec, "Altiris 7.0 Planning and Implementation Guide Version 1.2," 2011, http://www.symantec.com/business/support/resources/sites/BUSINESS/content/live/HOW_TO/9000/HOWTO9811/en_US/Altiris%207%20Planning%20%20Implementation%20Guide%20-%20v1%202.pdf.

communicate with core servers that store client data on SQL or Oracle database server(s). Software updates are deployed from each core server directly to each client. LDMS offers a two-tiered architecture, in which multiple core servers can synchronize or operate autonomously from a master core server.[186] Each core server is limited to a capacity of 25,000 clients. A rollup core server can be used to consolidate SQL data from multiple core servers to report on the status of up to 250,000 clients.[187] Permissions are handled by role-based access controls and patching is handled by the organic patch and compliance tool using client agents. LDMS supports Windows, Mac and Linux client OS's. In addition, it provides MDM support for iOS, Android, Blackberry and Windows mobile devices, but not patching support. LDMS allows for automatic update installation on collections of clients and even allows for peer-to-peer downloading of updates within the same subnet. LDMS also has an "auto fix" function for clients. Deploying updates with LDMS 9 requires a separate patch manager subscription.[188] In addition, certain functions related to the integrated patching process require the use of the Automated Lifecycle Management (ALM) module, which is included in the licensing costs.[189] If these components are used, LDMS has greater functionality than SCCM. A caution from Gartner was that a number of customers criticized LDMS 9 for issues with OS deployment, patch management and reporting quality.[190] This tool does not have the scalability to support Army or DoD requirements with a single hierarchy.

---

[186] LANDesk, "LANDesk Management Suite 9.0 Core Synchronization," *LANDesk Software Inc, 2012*, http://help.landesk.com/Topic/Index/ENU/LDMS/9.0/Content/Windows/sync_o_overview.htm.

[187] Frederick W. Broussard, Randy Perry and Tim Grieser, "Gaining Business Value and ROI with LANDesk Software: Automated Change and Configuration Management," *IDC*, January 2011, http://www.creekpointe.com/landesk/pdf/IDCBusinessValue.pdf.

[188] LANDesk, "LANDesk Management Suite 9.0 User's Guide," *LANDesk Software Inc.*, 2011, http://www.landesk.com/resources/product-documentation.aspx#ldms90, 305.

[189] LANDesk, "LANDesk Management Suite 9.0 Configuration the LANDesk Management Suite/ALM Patch Integration," *LANDesk Software Inc.*, 2009. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CEoQFjAC&url=http%3A%2F%2Fcommunity.landesk.com%2Fsupport%2Fservlet%2FJiveServlet%2Fdownload%2F5098-5-22975%2FLDMSPatchProcessIntegration90.pdf&ei=D2SDT531HKiQiQKQjtHjBQ&usg=AFQjCNFCFNS54kRuudMPFkgTz2xElKIJOQ&sig2=AFxJRukQ3l8pPVmwTfQxOg, 11.

[190] Cosgrove, *Magic Quadrant for Client Management Tools*.

5. IBM Tivoli Endpoint Manager (TEM)

IBM TEM is essentially a rebranding of the successful BigFix Enterprise Suite, which IBM acquired in July 2010. TEM consists of several modules including security and compliance, patch management, core protection, lifecycle management, power management and software use analysis. It makes use of both agent and agentless means of managing clients and conducting network scans. It also is capable of patching Microsoft, Mac, Unix and Linux OS's using a single agent. TEM has robust MDM capabilities for iOS and Android devices. It is the only tool evaluated that has dedicated agents for iOS and Android, which allows it to perform comprehensive CM functions on those devices, to include deploying "apps."[191] TEM is unique in its use of a proprietary *fixlet*[192] authoring language, which means that new administrators have an additional barrier to using the tool. TEM differentiates itself from other CM tools by its use of an "intelligent" agent. Agents inspect *fixlet* messages deployed by their TEM server to determine when their client is out of compliance and initiate remediation action without administrator involvement, which contrasts with most other tools that require administrators to scan for out of compliance clients and initiate action. Another unusual aspect of TEM is its scalability, which allows for each management server to support up to 250,000 endpoints.[193] As a result, TEM is marketed at large enterprises. The TEM architecture consists of four elements: TEM Server; TEM Relay(s), TEM Client and TEM Console. The TEM agent, located in each client, can either access a relay or server to receive updates. The purpose of the relay is to serve as a distribution point for load balancing purposes. To further aid in load balancing, relays can be organized into a hierarchy, with a top-level relay acting as the collection point for multiple child relays. A consolidated status of all TEM clients is available via the TEM console, which is not

[191] IBM, "Tivoli Endpoint Manager: Mobile Device Management," *IBM Software*, April 3, 2012, https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Mobile%20Devices%20Overview.

[192] *Fixlet* messages are individual policies to which each client must adhere. An individual *fixlet* message might require a client to have version 10.3.X.X. of Adobe Flash. The client would then attempt to retrieve this update from its relay.

[193] IBM, "Selecting the Right Solution for Endpoint Management," *IBM Software*, January 2012, http://public.dhe.ibm.com/common/ssi/ecm/en/tio14008usen/TIO14008USEN.PDF.

web-based. The architecture supports multiple servers, but only for backup purposes. Although the TEM server can support 250,000 clients, it is incapable of being tiered with another server, which limits a single hierarchy to 250,000 endpoints.[194]

6. HP Client Automation Enterprise (HPCA)

HPCA Enterprise is a desired-state CM tool designed for large enterprises with more than 10,000 clients. HPCA architecture consists of a single core server that maintains the authoritative data about all clients residing in the hierarchy. Satellite servers connect to the core server and provide access to HPCA resources for client devices. Satellite servers send their configuration data to their upstream source, which can be another satellite server. The data then makes its way to the core server. Due to this architecture, the core server can rebuild, add, or remove satellite servers at any time.[195] Satellite servers obtain new policies, patches and other data by synchronizing with their upstream satellite server or core server. When the client's agent determines that it requires a patch, it contacts its satellite server, which deploys the patch to the client.[196] The HPCA agent supports management of Windows, Linux and Mac clients, but only provides patching support for Windows, Red Hat and SuSE clients.[197] HPCA also provides driver and firmware support for HP devices. Unfortunately, HPCA does not provide any third-party patching capability, nor does HPCA documentation make any mention of creating third-party patches.[198] HP claims that HPCA provides unlimited scalability, but this is only the case when multiple core servers are used in a multi-hierarchy deployment. Interestingly, HPCA documentation fails to mention how many clients are supported by each core or satellite server. Gartner notes that HPCA has

---

[194] IBM, "Selecting the Right Solution for Endpoint Management."

[195] HP, "HP Client Automation Enterprise Edition for the Windows Operating System 8.10: Getting Started Guide," *Hewlett-Packard Development Company, L.P.*, February 2012, http://support.openview.hp.com/selfsolve/document/KM1332107/binary/CA8.10_CoreSat_GSG_Concepts.pdf?searchIdentifier=267d8d34%3a136a77065e3%3a476e&resultType=document.

[196] Ibid., 83.

[197] HP, "HP Client Automation Enterprise Patch Management for Windows and Linux Operating Systems 8.10," *Hewlett-Packard Development Company, L.P.*, February 2012, http://support.openview.hp.com/selfsolve/document/KM1332147/binary/CA8.10_PatchMgt_RG.pdf?searchIdentifier=267d8d34%3a136a77065e3%3a462d&resultType=document.

[198] Ibid., 16–26.

advanced bandwidth features and is highly scalable, but lacks MDM capability. It also found that HPCA is growing much slower than many of its competitors.[199] A significant shortcoming of HPCA is that it does not support any third-party patching. Another shortcoming of HPCA is that while HP supports the use of HPCA in a virtualized environment, the HP support organization does not support "the hypervisor (such as VMware ESX) or the host itself (such as VMware Server or Microsoft Virtual Server)."[200] These shortcomings are not encouraging and do not promote much confidence in using HPCA in a virtualized environment.

7. CFEngine 3

CFEngine 3 was devised originally to update Unix computers, and adapted over the course of nearly 20 years to provide management over a wider range of devices. Still, CFEngine 3 remains primarily a Unix/Linux/Mac focused product with the ability to manage Windows devices to a lesser extent.[201] CFEngine 3 comes in two editions, CFE Community and CFE Nova. CFE Community is a free, open source edition of CFEngine 3. CFE Nova provides commercial support for CFEngine 3 and improves its capabilities by providing native support for Windows, reporting, FIPS 140-2 compliance, LDAP integration, a GUI-based management console, virtualization support, and many other enhancements. This overview discusses CFE Nova, as it more closely aligns with Army needs. CFEngine 3 is a best of breed open source CM tool intended to manage the entire lifecycle of client devices. It was designed specifically to perform well on unreliable networks with low bandwidth, with client devices that lack significant processing power, which includes sensors or embedded devices. CFEngine 3 was also designed to work in ad hoc environments, with a premium placed on fault tolerance. CFEngine 3 is a desired-state tool, in which the agent in each client receives policy in the form of a "promise" file

---

[199] Cosgrove, *Magic Quadrant for Client Management Tools*.

[200] HP, "HPCA Platform Support Matrix," *Hewlett-Packard Development Company, L.P.*, November 11, 2011, http://support.openview.hp.com/selfsolve/document/KM1332718/binary/CA8.10_Support_Matrix.pdf?searchIdentifier=32ae5388%3a1370f5188b2%3a-710a&resultType=document.

[201] CFEngine, "CFEngine Quick Start Guide," 2012, https://cfengine.com/manuals/cf3-quickstart#!prettyPhoto[gal1]/1/.

from a policy distribution server. The client then requires no additional direction from the server to accomplish remediation. Clients always initiate contact with policy servers; changes are never pushed or forced to clients by servers. CFEngine 3 provides fewer features in comparison to most other CM tools, but does contain core CM functionality. It lacks MDM support and makes use of an open source Mongo database. CFEngine 3 source code was written in the CFEngine 3 software language, which means that implementing and operating this tool is significantly more complicated than commercially available tools.[202] In addition, making changes to clients always involves updating the promises.cf file. Updating that file requires writing code, which is something average system administrators do not know how to do. CFEngine 3 supports Windows, Mac, Linux, and Unix OS' for clients, but does not support Windows Server 2008 to host its policy server, which must run on Debian, Ubuntu, RHEL/CentOS or SLES/openSuSE.[203] The solution is scalable, and can make use of either a star or constellation topology. CFEngine 3 supports replication to downstream servers, but not autonomous mode.[204] Autonomy requires the creation of a new hierarchy. CFEngine is used by numerous high profile customers, including Facebook, AMD, AT&T, Chevron, Cisco, Ebay, FedEx, PayPal, IBM, Nokia, Shell, Juniper, MIT, Stanford University and many others.[205] Despite these impressive deployments, it does not appear this tool can support the enterprise scalability requirements of the U.S. Army or the DoD with a single hierarchy.

8. Local Update Publisher (LUP) for WSUS

Local Update Publisher (LUP) is not a CM tool. Instead, it can be thought of as an open source version of SCUP. Its purpose is to import, sign and approve custom updates for use on WSUS. In this way, updates for third-party applications can be created and

---

[202] CFEngine, "CFEngine Quick Start Guide."

[203] Ibid.

[204] Ibid.

[205] CFEngine, "CFEngine @ Work: Worldwide Customer Success," 2012, https://cfengine.com/use_cases.

published to WSUS using LUP for distribution to all clients supported by the WSUS hierarchy.[206]

LUP accomplishes the publishing of custom updates to WSUS by taking advantage of local publishing, which allows system administrators to create and publish custom updates to WSUS. By default, WSUS treats any updates that are locally published as unauthorized. In other words, although the update is locally published to WSUS, it is hidden from the WSUS console, which prevents the new update from being distributed. LUP partially solves this problem by providing its own very basic console to create, view, publish and approve third-party updates to WSUS, which is then used to distribute the custom updates along with the regular Microsoft updates. Update content consists of XML metadata, which contains the deployment logic for locating software that needs the patch, and the patch executable. It is unclear why Microsoft chose to hide locally published updates from the WSUS console.[207] One potential reason is that it could take business away from their SCCM line, as WSUS customers that want to patch third-party applications are normally recommended to pursue SCCM, which uses SCUP to publish updates to WSUS. When the authors contacted Microsoft about allowing the WSUS console to display locally published updates, the authors were informed that Microsoft "does not accept suggestions for new products, technologies or processes."[208] Using the LUP tool to author updates can be complex. Certain updates are quite simple to create, including updates for Adobe Flash. Other updates are considerably more difficult to build, which requires a significant amount of research and testing. Once a custom patch is built using LUP for a certain vendor's product, building follow-on packages becomes much easier, as vendors typically follow the same format when releasing follow-on patches. Still, the main limitation of LUP is that locally published updates do not appear on the WSUS console, which requires system administrators to use the LUP console to manage third-party updates.

---

[206] Local Update Publisher, "Local Update Publisher: Publish Your Own Updates to WSUS," 2010, http://localupdatepubl.sourceforge.net/index.html.

[207] Microsoft, "Local Publishing," (n.d.), http://msdn.microsoft.com/en-us/library/bb902470.

[208] Personal correspondence with Microsoft Customer Service Representative on April 25, 2012.

9. SolarWinds Patch Manager

SolarWinds recently acquired EminentWare, and is in the process of rebranding the EminentWare WSUS extension pack as SolarWinds Patch Manager (PM). SolarWinds PM represents the most complete extension of WSUS currently available. In addition to extending third-party patching to WSUS, it also provides a new GUI web-based console, WUA repair/reinstall, client inventory, reporting, and device discovery. Basic licensing costs include a subscription service that provides ready-made and tested third-party patches. Deploying patches is accomplished by deploying a SolarWinds server that integrates with WSUS. Each SolarWinds server can be associated with multiple WSUS servers. Not all WSUS servers need to be associated with a SolarWinds server; however, all WSUS servers operating in autonomous mode must be associated with a SolarWinds server. The SolarWinds server makes use of an agentless architecture to execute actions on client systems. Patch Manager only supports Windows clients, has minimal CM capability, and has no MDM capability. Notwithstanding, it takes advantage of the scalability of existing WSUS deployments to deploy third-party patches.[209] In addition, Patch Manager is easy to deploy, configure and put into operation in comparison to dedicated CM tools like SCCM, LANDesk and others. Ease of use is another strong point for Patch Manager because its console is so similar in layout to the WSUS console. Typical system administrators familiar with WSUS will be able to start making effective use of Patch Manager almost immediately.

10. eEye Retina CS with Patch Management Module

Retina CS is significantly different from each of the other tools in this analysis because it integrates vulnerability discovery, prioritization, and remediation reporting into a single tool.[210] Retina CS incorporates Retina NSS, which is currently approved as the Army's GNEC 6+1 network vulnerability scanner. Unfortunately, Retina NSS deployed under GNEC 6+1 is a stand-alone tool, which lacks any provisions for

[209] EminentWare, "Deploy and Manage 3rd Party Patches and Applications," http://www.eminentware.com/assets/pdfs/EminentWare-WSUS-Extension-Pack-005-Datasheet2.pdf.

[210] eEye Digital Security, "Retina CS Management Console," 2012, http://www.eeye.com/eEyeDigitalSecurity/media/Datasheets/Retina/Retina-CS-DS.pdf.

remediating clients after vulnerabilities have been discovered during scanning. Retina CS is a modular solution, with the capability to use three add-on modules: patch management, configuration compliance and regulatory reporting. The patch management module provides a subscription service for pre-packaged third-party updates.[211] Like SolarWinds Patch Manager, this tool only supports patching for Windows clients and uses an agentless model that leverages existing WSUS servers to deploy Microsoft and third-party updates, which is completed by deploying a separate Retina CS server. In addition to hosting the Retina NSS, the Retina CS server also utilizes a direct plug-in, which allows it to control the behavior of WSUS. The tool is scalable to at least three-tiers and allows rollup of data collected by Retina NSS at tier three to the Retina Compliance and Security Enterprise Management Console at the enterprise level.[212] Unlike SolarWinds Patch Manager, Retina CS supports vulnerability management for Blackberry, Android and ActiveSync-managed devices, although it cannot patch these devices.[213] In many regards, this solution is similar to the offering from SolarWinds in terms of third-party patching functionality. The value added from this solution is integration with Retina NSS, IAVM reporting and the capability to remediate vulnerabilities with a single tool using a single console, which represents a major capability improvement in comparison to other WSUS extension tools. One limitation of Retina CS is that its integrated scanner lacks the capability of conducting targeted scans of IP address or hostname lists, which is a feature that the standalone version of NSS contains.

G. FINAL CONTENDER ANALYSIS

1. Introduction

The purpose of this section is to determine how closely each of the contenders comes to meeting U.S. Army requirements for an optimal third-party patching tool.

[211] eEye Digital Security, "Retina CS Add-On: Patch Management Module," 2012, http://www.eeye.com/eEyeDigitalSecurity/media/Datasheets/Retina%20CS%20Add-Ons/Retina-CS-Patch-Mgmt-DS.pdf.

[212] eEye Digital Security, "Retina CS, Retina Insight Solution Briefing," 2011, http://www.youtube.com/watch?v=egWcwYYidxg&feature=relmfu.

[213] Ibid.

Vendor supplied documentation was used to determine individual tool capabilities. When this documentation was unavailable or insufficient, the authors used trial software of each tool in an attempt to determine capabilities. Testing of trial software was done in a virtual environment using VMware Workstation 8.0.1, hosted by a Window 7 Ultimate 64-bit workstation with a 2.66 GHZ Core i5 processor and 6GB of RAM. Within Workstation 8, each tool was installed on a virtual server running Windows Server 2008 R2, 64-bit, enterprise edition and joined to an AD domain. In addition, a three tier WSUS server hierarchy was established to simulate WSUS servers operating at the NETCOM, TNOSC and NOSC levels. Two VM clients running 32-bit and 64-bit versions of Windows 7 were used to aid in functionality testing. This testing was done to assess only basic tool functionality when documentation was unclear or unavailable. Tool performance criteria were not evaluated. Each of the evaluation areas in the following subsections includes a table showing the tool requirements, as identified previously in the chapter, along with the capabilities of each tool. Each requirement is prioritized from one to three. Priority one represents a mandatory requirement. Priority two represents an important requirement. Priority three represents a "nice to have" requirement. For the purposes of this analysis, LUP, SolarWinds Patch Manager and Retina CS are considered in the context of use with an established WSUS infrastructure.

2. Scalability and Architecture

Scalability was one of the largest differentiators between each of the tools (Table 2). Few tools available today scale to support organizations the size of the U.S. Army or the DoD with a single hierarchy. All the tools tested could scale to meet U.S. Army and DoD requirements if enough separate hierarchies were implemented, but that type of deployment introduces unnecessary and unwanted complexity. SCCM, Altiris CMS, LANDesk LDMS, IBM TEM and HPCA all fit into this category. SCCM 2012 can support up 400,000 clients in a single hierarchy and is the most scalable of the full featured CM tools in this analysis. SCCM 2012 would require at least two hierarchies' to support Army requirements. Meeting DoD requirements would be completely unfeasible as it would require at least 20 separate hierarchies. IBM TEM and LANDesk LDMS are the next most scalable tools with a single hierarchy supporting up to 250,000 clients.

Altiris CMS, HPCA[214], and CFEngine[215] all support less than 250,000 clients in a single hierarchy. Each of the WSUS-based tools, including the SolarWinds PM and Retina CS can, in theory, support U.S. Army and DoD requirements with a single hierarchy. Only a comprehensive field test could answer this concern with any degree of certainty. Most of the tools evaluated made use of a tiered hierarchy. Only IBM TEM made use of a single central server using only distribution points to connect clients, with no provision to tier configuration servers. Microsoft SCCM, HPCA, Altiris CMS, LDMS and CFEngine all make use of multiple tiers, each with a core or multiple core servers connected to at least one tier of child servers. SolarWinds PM, Retina CS and LUP rely on existing WSUS hierarchies, which in the Army, extend to at least three tiers.

All the tools support creating and distributing patches from the top tier. Only TEM lacks parent to child server replication due to its single server architecture.[216] Fewer tools support autonomous mode between parent and child servers. Only SCCM, Altiris CMS, LDMS, SolarWinds PM, Retina CS, and LUP allow child servers to choose what policy to accept from parents. CFEngine 3 allows for each server in the hierarchy to distribute a separate policy, but must be done manually for each server; by default, all clients and servers replicate policy with their parent server.

[214] HPCA documentation claimed the solution had “unlimited scalability,” but did not mention the maximum number of clients supported by a core server.

[215] CFEngine 3 also did not state the number of clients supported in a single deployment, but its architecture was consistent with support for 100,000 or fewer clients.

[216] TEM uses a single server model. Clients communicate with relays, which serve to reduce load on the core server.

SCALABILITY AND ARCHITECTURE TOOL REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Single Hierarchy Scalable to Army?	1							✓	✓	✓
Single Hierarchy Scalable to DoD?	2							✓	✓	✓
Tiered Architecture?	1	✓	✓	✓		✓	✓	✓	✓	✓
Create and Distribute Patches at Top Tier?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Child Servers Can Replicate Patch Content and Approvals From Parent?	1	✓	✓	✓		✓	✓	✓	✓	✓
Child Servers Can Operate Autonomously From Parent?	1	✓	✓	✓				✓	✓	✓

Table 2. Scalability and Architecture Requirements

3. Ease of Deployment and Use

Ease of deployment and use are critical factors in this analysis (Table 3). Ease of deployment is concerned with how difficult a tool is to put into operation enterprise-wide, especially at the NOSC level. A key consideration for each tool is adequate deployment planning prior to implementation. Even with adequate planning, no tool is simple to deploy on an enterprise level. With that said, all the tools hosted by Microsoft Server 2008 used fairly simple wizard-based installers. As mentioned previously, setting up the SQL database instance, especially a remote SQL instance, was the most significant installation challenge. The complexity in deploying each of these solutions is mostly a result of the configuration complexity after the basic installation is finished, especially when configuring certificate-based authentication. All the full featured CM tools add a degree of complexity to the configuration aspect of tool deployment because they require a unique agent to be installed on each client. The WSUS based tools make use of the WUA that all Windows-based clients come pre-installed with, which is a significant advantage for Retina CS, SolarWinds PM and LUP.

Microsoft SCCM and Altiris CMS are the most complicated of the Windows-hosted CM tools to deploy. They both require dedicated teams of specialists to deploy and configure, even at the TNOSC/NOSC level. The Army chose this course of action when it deployed Altiris to USARPAC prior to the rollout of SCCM. It is also the reason the Army contracted Microsoft to deploy SCCM Army-wide,[217] which is one of the major shortcomings of this type of solution. IBM TEM is the simplest of the traditional CM tools to put into operation because it requires only a single core and multiple relays at individual sites. Expansion from the core only requires new sites to add relays, which can reside on existing desktops or servers that make this tool easy to expand. As a bonus, relays do not have to contain a database connection; only a connection to the core server. Deployment of LDMS would most likely necessitate deploying at least one core server to each camp/post due to the core server capacity of 25,000 clients. As a result of LDMS's peer-peer capability, it would be possible for clients to connect to off-site core servers. Clients that connect in this way effectively become distribution servers within their subnet and reduce core server load. HPCA also uses a core server, and offers the advantage of easily replicating or deleting child servers because all data is stored by the core database. In other words, provisioning new satellite severs, such as at a new post, could be done at the enterprise (NETCOM) level once hardware was allocated. Unfortunately, child servers cannot be hosted on virtual servers. CFEngine 3 is easily the most difficult CM tool to deploy because it is the only tool that does not use a Microsoft Server OS as its host, or a SQL database. Few system administrators in the Army are familiar with Linux servers, especially at the NOSC level.

In contrast to the dedicated CM tools, each of the WSUS-based tools takes advantage of an existing WSUS infrastructure, which is a significant advantage for organizations like the U.S. Army and the DoD, which embraced WSUS. One significant deployment advantage is that each tool takes advantage of the existing WUA agent that is already configured and deployed for use by WSUS. In addition, each of the WSUS-based tools requires a download of less than 600 MB for installation that is much less than the

[217] Microsoft, *Performance Work Statement for United States Army Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM/9th SC (A)), Enterprise Systems Technology Activity (ETSA) For Microsoft Consulting Services for Systems Management (SysMan) Sustainment Support*.

full featured CM tools, with the exception of IBM TEM, which is a small 250 MB download. Each WSUS-based tool offers a relatively simple setup and configuration process, as long as a WSUS infrastructure is already in place. LUP is the easiest of all the tools to deploy and configure by a wide margin. The download is less than 1MB, and installation and configuration can be done is less than an hour, which is mostly because the tool's functionality is so limited in scope. SolarWinds PM and Retina CS are both fairly simple to install and configure, although most system administrators will find SolarWinds slightly less complex. Most of the setup difficulty with SolarWinds PM and Retina CS revolve around database installation and setup, which is major chore for the entire range of CM tools, with the exception of LUP.

Most of the tools can be hosted by a virtual server; however, HPCA does not support VM use in production environments and Altiris CMS does not support virtualization in environments with over 10,000 clients. Other vendors stress ensuring minimum requirements are met while installing their tool on a virtualized server. Each vendor supplied detailed documentation for its tool; however, HPCA was the most difficult to locate. Detailed documentation from eEye could only be obtained by contacting its sales department. Several vendors offered a wide range of useful videos, including Microsoft, LANDesk, CFEngine, SolarWinds and eEye. Of those, Microsoft offered the most extensive and useful video tutorials. In addition, Microsoft SCCM has a very active online user community that makes finding solutions to common problems easy in comparison to other CM tools.

Evaluating ease of use is highly subjective. In general, the more complex tools are also the most challenging to learn to use quickly. CFEngine 3 is the most difficult to use because system administrators must learn CFEngine 3 programming to create the *promise.cf* configuration files distributed to each client. SCCM, Altiris CMS, LANDesk LDMS, IBM TEM and HPCA all have a plethora of features. Only the most gifted system administrators could hope to achieve basic proficiency in only a few days of training. SolarWinds PM is the simplest of the tools to operate, as its functionality is centered on patching and the console is very similar to that of WSUS. Retina CS is more complex than SolarWinds PM, but less so than the full featured CM tools, which mostly

results because Retina CS uses a dedicated vulnerability scanner, which is not available with any other tool. LUP is very simple to use, so long as an .msi update file is provided by the third-party vendor to aid in custom patch creation. The .msi file contains the detection logic for patch deployment to Windows clients, which makes using the update creation wizard in LUP very easy. Without the .msi file, patch creation can be very difficult. Patches, such as those for Adobe Flash, which offer an .msi file, can be created and approved in less than five minutes. Ease of use is hampered, however, because LUP does not integrate fully with WSUS, which requires the system administrator to work on two separate consoles.[218]

Each of the tools in the analysis made primary use of a GUI web console, although SCCM, TEM and SolarWinds PM did not support accessing their tools from a web browser. All tools supported some degree of CLI input. All tools, with the exception of CFEngine 3, supported at a minimum, Microsoft Server 2008 and SQL Server 2008 as their host operating system and database engine, respectively.

[218] Updates published by LUP to WSUS are hidden in the WSUS console, requiring the use of the LUP console to publish updates and monitor the status of client update installations.

DEPLOYMENT & USE TOOL REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Average NOSC Admin Capable of Deployment and Configuration?	1				✓	✓		✓	✓	✓
Requires Less Than Eight hrs Formal Training and Less Than Three Days OJT for Basic Tool Operation?	1							✓	✓	
Tool Can be Hosted by a VM Server?	2	✓		✓	✓		✓	✓	✓	✓
Highly Detailed Documentation?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
GUI Based Console?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Control Tool From Web Browser?	2		✓	✓		✓	✓		✓	
Supports MS Server 2008 and SQL Server 2008?	2	✓	✓	✓	✓	✓		✓	✓	✓
10-Minute Tutorial Video?	3	✓		✓			✓	✓	✓	
CLI Console Support?	3	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 3. Deployment and Use Tool Requirements

4. Functional Capability

Automated deployment of third-party patches was a key requirement for these tools and it was one area with little divergence (Table 4). All tools, with the exception of HPCA, supported this requirement. With CFEngine 3, a policy must be created for each patch, which requires each client to contact a server to obtain the update. LDMS requires the patch manager add-on, while Retina CS requires the patch management add-on to enable third-party updating. Both of those add-ons are included in this analysis. SolarWinds Patch Manager includes access to a wide range of pre-tested third-party patches as part of the licensing costs. All the CM tools, with the exception of CFEngine 3, pull Microsoft updates directly from Microsoft's own update catalog. Most full featured CM tools included patching support for Windows, Mac, Linux and Unix; however, SCCM, SolarWinds PM and Retina CS only patch Windows clients. None of the tools were capable of deploying updates to mobile devices or networking devices. At this point, MDM consists primarily of monitoring usage and analyzing vulnerabilities, but not remediating vulnerabilities. None of the tools can natively manage network

devices, although SCCM can use the QMX third-party plug in to gain this capability. Each of the tools incorporated some type of detection logic that allowed either the client's agent, or the management server, to determine if a patch was required.

Each tool interfaced with AD, which it could leverage to deploy agents using group policy. Some tools, including SCCM, LDMS and TEM, had the capability to quarantine misconfigured clients or were missing critical updates. LDMS and SolarWinds PM had the capability to automate the repair of misbehaving agents. Other tools lacked the capability and would require an add-on to automate this process.

All the tools tested supported some type of RBAC to delegate permissions to administrators. Most tools also made use of PKI to ensure client to server communications were authentic, although CFEngine lacked this capability. All the tools supported some level of reporting, which included report rollups to the top of the server hierarchy. Only HPCA and Retina CS were capable of generating IAVM specific reports. Finally and not surprisingly, only Retina CS integrated with the Retina NSS, which represents a significant advantage over the other tools. Finally, all the tools made use of some form of client agent. Each of the full featured CM tools used a specialized agent that must be installed on clients as part of the configuration processes. Each of the WSUS-based tools made use of the WUA client that is integrated with all Windows devices.

FUNCTIONAL TOOL REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Automated Third-Party Patch Deployment For Designated Collections?	1	✓	✓	✓	✓		✓	✓	✓	✓
Built-in Detection Logic?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Uses Certificate Based Authentication (PKI)?	1	✓	✓	✓	✓	✓		✓	✓	✓
Supports Role Based Assignment of Admin Permissions?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integration With eEye Retina NSS?	1								✓	
Uses Client Agent?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Patches Mac, Unix, Linux?	2		✓	✓	✓		✓			
Update Mobile Devices: Android, iOS, Blackberry?	2									
Interfaces with MS AD?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automated Repair of Misbehaving Agents?	2			✓				✓		
Prevent User from Cancelling Patch Install?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supports Client Grouping by Type, OS, and Functional Designation?	2	✓	✓	✓	✓	✓		✓	✓	✓
Generate IAVM Compliance Reports?	2					✓			✓	
Report Rollups Avaiable at Top Tier?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Update Networking Devices?	3									
Quarantine Out of Compliance Clients?	3	✓			✓					
Agent Deployment Using AD Group Policy?	3	✓	✓	✓	✓	✓		✓	✓	✓
Agent Check-In Frequency Adjustable?	3	✓	✓	✓	✓	✓	✓		✓	
Allow User to Delay Patch Installation?	3	✓	✓	✓	✓					

Table 4. Tool Functional Requirements

5. Interoperability

The capability to support the entire DoD under a single hierarchy was the key criteria the tool had to meet to support interoperability (Table 5). Only the tools that leveraged WSUS have the potential to meet this key requirement. LUP accomplished this by simply allowing custom updates to be published to a top-level WSUS. Retina CS and SolarWinds PM met the requirement by integrating their own servers into the WSUS hierarchy. The remaining tools were held back by the number of clients that a single hierarchy could support. The other requirements for bandwidth throttling and functioning in a low bandwidth environment were supported by each of the tools.

TOOL INTEROPERABILITY REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Can Function Properly on Unstable Networks With Low Bandwidth?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supports Bandwidth Control?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Could Potentially Provide a DoD-Wide Third-Party Patching Solution?*	2							✓	✓	✓

Table 5. Tool Interoperability Requirements

6. Regulatory Guidance

Each of the tools evaluated is capable of meeting current regulatory requirements under FIPS 140-2, and CCEVS (Table 6) because all the tools, with the exception of CFEngine 3, can be hosted by Windows Server 2008, which is certified under FIPS 140-2 and CCEVS. CFEngine 3 can be hosted on the Linux RedHat OS, which is also certified under FIPS and CCEVS.[219] [220] Each of these tools is capable of meeting CON requirements under specific conditions, such as use by a specific TNOSC, as was the case with Altiris when it was deployed by the PTNOSC, which is the case because aside from meeting regulatory guidance under FIPS and CCEVS, awarding a CON is based on meeting NetOps objectives that can be unique to different organizations. All tools except for LUP meet the requirement under AR 25-2 to record logon attempts and track user logon data. LUP does not require any user authentication beyond having administrative rights on the server hosting LUP.

[219] National Institute of Standards and Technology, "FIPS 140-1 and FIPS 140-2 Vendor List," 2012, http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

[220] National Information Assurance Partnership, "Validated Products List," 2012, http://www.niap-ccevs.org/vpl/.

TOOL REGULATORY REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Meets FIPS 140-2?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Meets CCEVS?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Capable of Meeting Army CON Requirements?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tracks Logon Attempts?	2	✓	✓	✓	✓	✓	✓	✓	✓	
Maintains User Logon Data?	2	✓	✓	✓	✓	✓	✓	✓	✓	

Table 6. Tool Regulatory Requirements

7. Reliability and Performance

The reliability and performance of these tools cannot be properly evaluated without a large-scale field evaluation of each product. Table 7 shows the requirements results for each tool as primarily blank since these requirements were not evaluated. Unlike scalability, performance and reliability cannot be reasonably gauged by examining the architecture of a tool. Each of these tools can be expected to perform adequately under the light load generated by limited laboratory testing. All vendors, with the exception of the open source LUP tool, have a plan in place for continued support of their tools. Of these, Symantec's support for Altiris CMS is questionable, as they laid off the original development team and relocated software development to low cost centers in India and Estonia.[221]

[221] Andrew Colley, "Symantec Australia to Shutter Software Unit," *The Australian*, June 8, 2011, http://www.theaustralian.com.au/australian-it/symantec-australia-to-shutter-software-unit/story-e6frgakx-1226071891896.

TOOL RELIABILITY AND PERFORMANCE REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Vendor Has Support Plan for Tool?	1	✓	✓	✓	✓	✓	✓	✓	✓	
Capable of 99.9% Uptime?	2									
Capable of 95% First Pass Patch Deployment Success Rate?	2									
Responsive Console?	2									
Capacity Client Load Decreases Server Performance by 20% or Less?	2									

Table 7. Tool Reliability and Performance Requirements

8. Cost

The cost of each tool is explored in-depth in the next section.

H. COST-BENEFIT ANALYSIS OF FINAL CONTENDERS

1. Introduction

What is an effective Cost-Benefit Analysis? As noted early in Chapter II, a CBA is used to evaluate the total anticipated cost of a project or product compared to the total expected benefits to determine whether the proposed implementation is worthwhile for an entity. CBA use was first mandated in the U.S. Federal government with Executive Order 12291, issued by President Reagan in early 1981.[222] If the results of this comparative evaluation method suggest that the overall benefits associated with a proposed action outweigh the incurred costs, then a business or project manager will most likely choose to continue with implementation.

Generally speaking, a CBA consists of three parts. First, all potential costs incurred by implementing a proposed action must be identified. Second, all anticipated benefits must be associated with potential actions. This study uses the costs that the U.S.

[222] Ronald Reagan, Executive Order no. 12291, *Federal Regulation*, National Archives and Records Administration Federal Register, February 17, 1981.

Army would incur to fix and repair computers and or networks affected by malware or viruses that exploited third-party application vulnerabilities. The final step is to subtract all identified costs from the expected benefits to determine whether the positive benefits outweigh the negative costs.

a. Identifying Costs

The first step in the CBA is to quantify all costs associated with a proposed action. All potential costs of implementing a given software application must be identified, which includes up-front costs incurred upon implementation and throughout the expected life cycle of the software application. For instance, start-up fees, licenses, production materials, user acceptance processes, training and continuing training are included.

b. Identifying Benefits

The second step in the CBA is to determine all the benefits derived from purchasing the proposed process or product. In his article, "Is There a Business Case for IT Security," Tom Pisello mentions that both the Computer Security Institute and the FBI report that as many as 82% of private organizations have suffered a malicious code attack, which is the most frequent type of security breach and the one most likely to cause financial damage.[223] The most recent CSI Computer Crime and Security Survey reported that malware infections continued to be the most commonly seen attack, with 67.1% of respondents reporting at least one incident during the year.[224] This number is staggering considering the increased security measures and amount of money spent by many organizations in an attempt to prevent cyber crime. Pisello suggests that each attack takes an average of four hours per system to fix, and costs about $24,000 per incident. This study utilizes $24,000 as the cost that would have been spent to remediate the adverse impacts of one malware infection. The remediation effort is assumed to be completed by

[223] Tom Pisello, "Is There a Business Case for IT Security*?" Security Management*, 2004, http://www.securitymanagement.com/article/there-business-case-it-security.

[224] Robert Richardson, "2010/2011 CSI Computer Crime and Security Survey," *Computer Security Institute*.

unit level, or NOSC system administrators on an installation. This CBA does not include costs that are very difficult to quantify, such as employee productivity losses, and lost IT personnel hours due to mitigation or remediation actions.

Government federal agencies are required to use a real rate of return of 7% with the assumption that it measures the before tax rate of return for the private sector. This analysis utilizes the 2009 discount value of 3.3% in calculating the future dollar values and takes into account inflation for future dollars.

2. Cost Benefit Analysis Steps

The basic steps of a CBA are designed to fit just about any project or product being analyzing. As a result, steps can be omitted or adjusted to fit the specific situation or product analyzed. These steps assist or lead a manager or purchaser to a recommended course of action based on constraints, given factors, and costs/benefits associated with each alternative action. As defined by Boardman,[225] the nine steps of the CBA are the following.

- Specify the set of alternatives
- Decide whose benefits and costs count (standing)
- Catalogue the impacts and select measurement indicators
- Predict the impacts quantitatively over the life of the project
- Monetize (attach dollar values to) all impacts
- Discount benefits and costs to obtain present values
- Compute the NPV of each alternative
- Perform sensitivity analysis
- Make a recommendation

3. Identify all Alternatives

According to Boardman, the first step in the CBA is to identify all alternatives.[226] The eight alternatives to SCCM 2012 have previously been identified and thoroughly

[225] Anthony Boardman, David Weimer, Aidan R. Vining, and David Greenberg, *Cost-Benefit Analysis: Concepts and Practice*, 3rd ed. (New Jersey: Prentice Hall, 2005).

[226] Boardman, Weimer, Vining, and Greenberg, *Cost-Benefit Analysis: Concepts and Practice*, 7.

discussed in the system engineering portion of the analysis and include Symantec CMS, LANDesk LDMS, IBM TEM, HP HPCA, CFEngine 3, SolarWinds PM, Retina CS and LUP.

4. Relevant Benefits and Costs

Step two of the CBA requires that the analyst decide who has standing or whose benefits and costs should be counted.[227] This step helps to identify the key players and stakeholders and define their role in the decision-making process.

a. Key Players

Understanding who the key players are in this analysis helps to establish the relationship each player has with the decision alternatives, as well as which role in the decision process. When analyzing the key players, this CBA examines two main factors that directly affect the decision-making process. As with any CBA, the two main factors to consider are cost and benefit. Table 8 shows both the influence and interest shown by each stakeholder, but goes further by demonstrating the financial and operational impact to each stakeholder.

STAKEHOLDER	INFLUENCE	INTEREST	ROLE	FINANCIAL IMPACT	OPERATIONAL IMPACT
Unit Level SA	Low	High	Customer	None	Positive
NOSC	Low	High	Customer	None	Positive
TNOSC	Medium	High	Customer	None	Positive
NETCOM	High	High	Decision Maker	Increase/Decrease	Negative
Microsoft	Low	High	Supplier	Increase/Decrease	None
Symantec	Low	High	Supplier	Increase	None
LANDesk	Low	High	Supplier	Increase	None
IBM	Low	High	Supplier	Increase	None
HP	Low	High	Supplier	Increase	None
CFEngine	Low	High	Supplier	Increase	None
SolarWinds	Low	High	Supplier	Increase	None
eEye Digital Security	Low	High	Supplier	Increase	None
LUP	Low	High	Supplier	None	None

Table 8. Stakeholder Analysis

[227] Boardman, Weimer, Vining, and Greenberg, *Cost-Benefit Analysis: Concepts and Practice*.

b. Key Stakeholders

The key stakeholder analysis is conducted to describe the influence, interest and role of each stakeholder, as well as the effects if a vendor other than Microsoft SCCM 2012 is selected as the best alternative.

Unit level IT system administrators are deemed to have a low influence over the choice of alternatives because they are at Tier 3 and low on the decision- making totem pole. U.S. Army installation NEC will be directly affected by the outcome of the choice from the alternatives, which requires the installation's NEC to adjust to the decision once it is made. Financial impacts at this level are minimal as the U.S. Army will make allowances for every system in the network at no cost to the end customer. Interest is high as unit level SA's workload will potentially decrease as a result of having another tool to utilize to mitigate software vulnerabilities. As such, the operational impact will be a positive one.

Installation level IT system administrators working at the NOC/NOSC level are also deemed to have a low influence over the choice of alternatives. However, the NEC's NOSC will be judged to have an increased influence if any negative outcomes associated with the selection of an alternative are found. Again, no impact to financials at this level as the U.S. Army will have included all systems in the licensing agreement. The NOSC is extremely interested in which alternative is selected as it will directly impact how it conducts business as a result, either positively or negatively. For instance, the selected platform could require additional instruction on a particular software language, such as CFEngine 3. As such, the operational impact will be a positive one in the long run.

Since U.S. Army TNOSC's are responsible for the network management and computer network defense for the Army's networks in a specific functional theater of operations, they have a medium influence on the decision. Like the previous two stakeholders, a financial impact beyond required training, if warranted, would not occur. The TNOSC will be highly interested in which alternative is selected as the decision will affect not only the software engineers and IT systems at Tier 2, but those at Tier 3 as

well. The operational impact will be positive and will fulfill the LandWarNet NetOps Architecture requirements and provide for a more secure network.

NETCOM has the highest influence out of all the stakeholders as it is at the Tier 1 level in the network. It serves as a key decision maker when it comes to making choices on what NetOps tools to deploy to operate and defend the LWN. At this level, based on the best choice of vendors, a financial impact may or may not occur. Bottom line, if the best choice meets Army requirements and is not the current solution, then the selected vendor may be more expensive or could be cheaper than the current solution. A negative operational impact is assumed as the changes would require oversight and management of the new remediation solution.

Each supplier of services and software to the U.S. Army, to include Microsoft, Symantec, LANDesk, IBM, HP, CFEngine, SolarWinds, eEye and LUP, has a low influence on the decision-making process that NETCOM will undertake. Microsoft has a high level of interest in maintaining the current third-party mitigation solution relationship it enjoys with the U.S. Army. Each of the other suppliers has a high interest in generating a business relationship with the U.S. Army. The financial impact to Microsoft will depend on many factors. Impact in the short run will not occur as SCCM 2007 has already been implemented by the U.S. Army, but perhaps in the long run, if SCCM 2012 does not perform as advertised, it could be replaced by a more robust remediation solution. Each of the other suppliers, with the exception of LUP, will experience an increased financial impact if selected and "courted" as the best choice as a remediation management solution. LUP will not experience an increased financial impact because the software is provided free of charge. None of the supplier services or solutions is expected to generate an operational impact.

5. Catalogue the Impacts and Select Measurement Indicators

Step three of the CBA requires the completion of two different tasks. First, the physical impact of alternatives must be listed as either a benefit or a cost. Second, this CBA will then specify the impacts' measurement units.[228] Impacts and measurement

[228] Boardman, Weimer, Vining, and Greenberg, *Cost-Benefit Analysis: Concepts and Practice*.

indicators for the eight alternatives analyzed for this CBA are divided into two different categories. The costs and benefits are the following.

- Software/licenses costs
- Remediating infections benefits

a. Software/License Costs

This study focuses on the actual costs incurred from purchasing the software and associated licenses. By far, the most time consuming process in this endeavor was reaching out to the vendors identified by the system engineering analysis. Most of the quotes were requested directly from each manufacturer/vendor of the individual remediation software. All the quotes received reflect retail pricing of tool licensing and support, with the exception of HPCA, which included a very significant discount. By requesting a five-year licensing and support period, several vendors provided additional discounts based on longevity. Vendor supplied quotes were normalized to the following specifications.

- Two server licenses
- 10,000 clients licenses
- Associated first year deployment costs (if any)
- Five-year service/support contract with upgrade

This analysis purposely did not include any costs incurred by acquiring additional infrastructure (if required), such as servers or the increased personnel costs associated with an individual product (if warranted). It is important to realize that one or more of the vendors could possibly require significant operator training to get systems up and running and maintained. These costs are not trivial, and are significant to the decision-making process; however, they will not be addressed within the scope of this study.

b. Benefits of Remediating Malware Infection

It has been argued that difficulties in quantifying benefits associated with improved information availability and decision making prevents effective IT CBA. For instance, measuring the percentage of third-party application vulnerabilities for which

patches have been applied or that have been otherwise mitigated is both an implementation and effectiveness measure. NIST SP 800-53 identifies measurements of implementation for the security control entitled "Flaw Remediation" (SI-2) or "Malicious Code Protection" (SI-3).[229] This publication has many different measuring tools within the system and information integrity that would prove useful to any organization looking for measurements to utilize in an effectiveness study. Effectiveness measures provide key information for information security decision makers about the results of previous policy and acquisition decisions. Most of the vendor products analyzed within this study have many options or features required to be considered in the analysis. Many of these options or features could also be utilized to measure effectiveness, which include the following security controls: "Incident Monitoring (IR-5), "Audit Monitoring, Analysis, and Reporting" (AU-6), and "Monitoring Configuration Changes (CM-4)." However, even though limited testing of most of the vendor's software in this study was conducted, it is simply not within the scope of this study to capture the data necessary to catalog the effectiveness of these measures. As can be seen from Figure 27, no single, prevalent method of determining whether a given security program is effective exists.[230]

[229] National Institute of Standards and Technology, "Recommended Security Controls for Federal Information Systems and Organizations: NIST Special Publication 800–53," *NIST*, Gaithersburg, MD, August 2009, http://purl.access.gpo.gov/GPO/LPS117689.

[230] Richardson, "2010/2011 CSI Computer Crime and Security Survey."

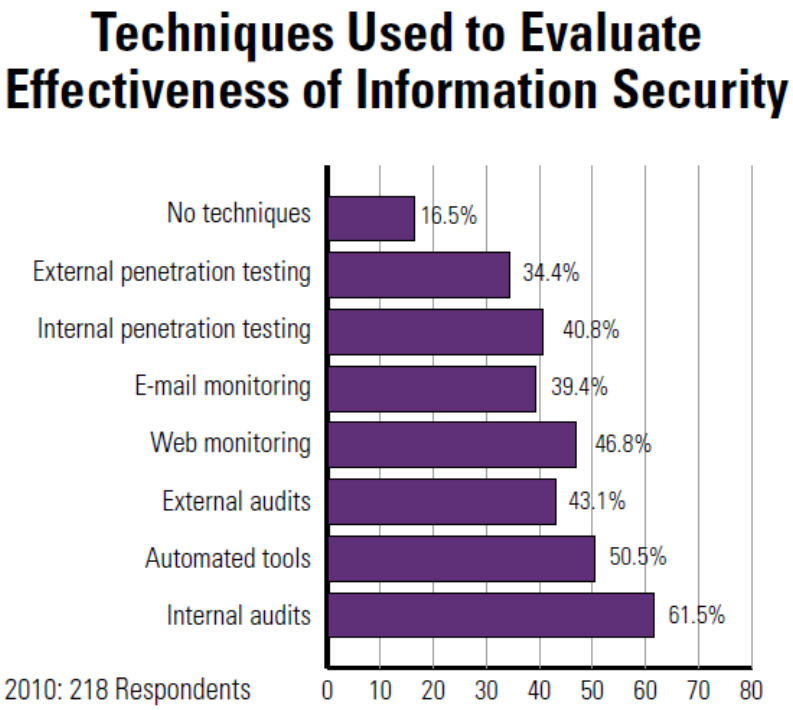


Figure 27. Effectiveness of Information Security[231]

Quantifying/monetizing an attack is also extremely difficult. Corporations have no incentives to reveal such information, which is a primary reason why comprehensive data on information security breaches are lacking. In fact, the Computer Security Institute stopped publishing the cost of cyber security incidents after its 2009 report due to a lack of participation from respondents.[232] Revealing this information may cost organizations even more than the actual attack due to a loss of trust in the organization. For instance, a company or corporation traded on any of the stock or credit markets may react negatively to reported security breach announcements. Company reputation or confidence in that company is affected negatively in relation to the market. Companies or corporations could face litigation by its investors, customers or other stakeholders to seek recovery of damages. For instance, if a health care provider is compromised, or its database, with Personally Identifiable Information (PII), or more

[231] Richardson, "2010/2011 CSI Computer Crime and Security Survey."

[232] Ibid.

importantly, health related information is breached, liability issues or concerns may arise. Most importantly, companies fail to report breaches because this would be a sign to the attackers that their cyber defenses are weak and could potentially inspire further attacks.

It is for this reason that this study utilizes a fixed remediation cost of $24,000 instead of attempting to monetize the hourly wages paid by the U.S. Army to contractors, which would vary greatly at each level within the LWN.[233] This cost is used to quantify the benefit of utilizing any or all of the selected software solutions, with the assumption that use of the third-party patching tool potentially prevents Army information systems from being compromised by malicious code, and results in zero dollars being spent on remediation efforts.

To quantify the benefit realized per attack by not having to remediate infected systems, a prediction must be made to estimate how often attacks are prevented. This study normalizes the cyber attacks prevented for all the vendors by using the same figures for each of the five years of tool use. This study does not attempt to predict accurately with any certainty the actual number of malicious code attacks actually experienced per 1,000 users. Pisello suggests using the following formula to predict the number of malicious code breaches attempted per year:

number of breaches per year = personal probability of security breach occurring × estimated number of incidents per 1,000 users × the multiple of 1,000 users.

A steadily decreasing percentage of the predicted number of breaches per year is used by starting with a 75% chance, to 50% then 25% for the last two years.[234] The actual number of breaches per 1,000 users gradually decreases, which reflects a more secure network due to the use of remediation efforts. The analysis first starts with 2.1 breaches per 1,000 users, then 1.9 per 1,000, 1.5 per 1,000, and finally, 1 breach per 1,000 users. The authors cannot assume a 100% secure network as Army networks will continue to experience attacks via successful phishing expeditions as users will continue

[233] Pisello, “Is There a Business Case for IT Security?”

[234] Ibid.

to click on unsafe links within emails or be lured to infected websites. As can be expected, the benefit realized each year decreases. This cyber risk cost model is very similar to an older Annual Loss Expectancy (ALE) developed in the late 1970s at the National Institute for Standards and Technology (NIST).[235] ALE has become a standard unit of measure for talking about the cost of cyber attacks, but the model is not universally used to assess cyber risk.

6. Predict the Impacts Quantitatively Over the Life of the Project

Step four of a CBA is to quantify all impacts for each alternative in each time period (i.e., over the life of the project). This analysis utilizes a five-year time period as most U.S. Army contracts are for at least three years. Ideally, the Army would commit to a five-year contract as the life-cycle of most information systems is limited to five years. For the purposes of this study, this particular step is addressed in two future steps in greater detail.

7. Monetize (Attach Dollar Values to) All Impacts

The fifth step of a CBA is to monetize each of the impacts identified in step three.[236] The impacts to be monetized and totaled for each alternative are related to the costs and benefits. The benefits calculated over a five-year period for all the tools analyzed were the same, at $756,000. All the quotes received reflected retail pricing, with the exception of the quote from HP, which reflected a 50% software discount and a 20% support discount. This study assumes that if the U.S. Army pursued a course of action recommended via this study that government pricing would be utilized in attaining a long-term contract. Table 9 shows the quote amount received from each vendor for the five-year period of support by assuming two server licenses, 10,000 client licenses, and any vendor deployment costs, as outlined previously.

---

[235] U.S. Library of Congress, Congressional Research Service, *The Economic Impact of Cyber-Attacks*, by Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, CRS Report RL32331 (Washington, DC: Office of Congressional Information and Publishing April 1, 2004), http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[236] Boardman, Weimer, Vining, and Greenberg, *Cost-Benefit Analysis: Concepts and Practice*.

MONETIZE ALL IMPACTS	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
5 Year Benefit	$756,000	$756,000	$756,000	$756,000	$756,000	$756,000	$756,000	$756,000	$756,000
5 Year Cost	$1,016,667	$1,696,500	$968,000	$1,270,000	$1,441,779	$4,014,000	$53,991	$328,780	$0
Quote Received From?	Vendor Website	Account Rep	Account Rep	Account Rep	Account Rep	Account Rep	Account Rep	Account Rep	N/A
Discount Pricing?	No	No	No	No	Yes	No	No	No	N/A

Table 9. Monetized Impacts for Each Tool

8. Discount Benefits and Costs to Obtain Present Values

The sixth step of a CBA is to discount each of the benefits and costs identified in the previous step. For a project that has costs or benefits that accrue over extended periods (years) as this study does, a need exists to aggregate the benefits and costs that arise in different years. Normally in a CBA, future benefits and costs are discounted relative to present benefits and costs to obtain their present values due to the Army's preference to consume now rather than later. Consumption now usually results in the expenditure of resources, which comes with an opportunity cost. To determine the present value of the money properly that is allocated for expenditure, the value of future dollars must be determined by using a "discount rate." This study utilizes a discount rate of 3.3% from the year 2009, which is published in Appendix B of OMB Circular A-94.[237]

The method used by this study to illustrate the discounting of costs and benefits is as follows. The cost or benefit that occurs in year t is converted to its present value (*PV*) by dividing it by $(1+d)^t$, where d is the discount rate. This study has a life of five years, so n=5. B_t and C_t are denoted as the benefits and costs in year t, respectively. The formula for this process is as follows:

$$PV(B) = \sum_{t=0}^{n} \frac{B_t}{(1+d)^t} \qquad PV(C) = \sum_{t=0}^{n} \frac{C_t}{(1+d)^t}$$

[237] Office of Management and Budget, *Guidelines and Discount rate for Benefit-Cost Analysis of Federal Programs*.

Microsoft Excel was utilized to compute the present values of benefits and costs, as well as the NPV. The results are displayed in Tables 10 and 11.

9. Compute the Net Present Value of Each Alternative

The seventh step in the CBA is computing the NPV of each alternative. The NPV of an alternative equals the difference between the present value of the benefits and the present value of the costs. The formula for this process is as follows.

$$NPV = PV(B) - PV(C)$$

In a CBA, when more than one alternative to the status quo exists and all the alternatives are distinct from each other, then the logical selection for the decision maker is the alternative with the highest/largest NPV. Thus, selecting the alternative with the highest/largest NPV is equivalent to selecting the alternative with the highest/largest present value of the net benefits. Normally in a CBA, a sensitivity analysis is conducted prior to making a decision on a course of action. However, because it is nearly impossible to predict and monetize all the costs and benefits as identified within this study, the authors acknowledge that the totals are not 100% accurate, but are close enough for a decision to be made. As a result, this CBA does not include a sensitivity analysis.

10. Perform Sensitivity Analysis

The eighth step in the CBA is to conduct a sensitivity analysis, which is omitted.

11. Make a Recommendation

The final step in the CBA process is to recommend the adoption of the alternative with the highest NPV. As mentioned earlier in the section, the NPVs are predicted values, and as such, the sensitivity analysis was unwarranted in this study. It is also important to note that CBA analysts make recommendations, not decisions. CBAs help managers discern how resources should be allocated in a more efficient manner.

The authors have included other measures of "success" commonly utilized in a financial investment across all businesses, which include the ROI and the Internal Rate of Return (IRR). ROI is a performance measure used to evaluate the efficiency of an

investment or to compare the efficiency of a number of different financial investments. To calculate ROI, the benefit (return) of an investment is divided by the cost of the investment, and the result is expressed as a percentage or a ratio. If the return in this case is less than the investment than the result will return a negative number and will not be useful in this study. The IRR uses a discount rate and is often used in capital budgeting that makes the NPV of all cash flows from a particular project equal to zero, which helps to ascertain the break even discount rate needed. Generally speaking, the higher a project's IRR, the more desirable it is to undertake the project. As such, IRR can be used to rank several prospective projects a manager is considering, especially if the projects are dissimilar. Assuming all other factors are equal among the various projects, the project with the highest IRR would probably be considered the best and undertaken first. As mentioned with ROI, the IRR will return a negative number if the costs are greater than the benefits. In this study, a zero will be utilized instead of the negative number. Arguments have occurred concerning whether ROI and IRR may not be ideal in determining which alternative to select because of uncertainties that usually happen in the business sector, which are included to illustrate that NPV is not the only tool that can be used in a CBA; however, it is the most appropriate tool to use in this study.

The alternative that had the highest/largest NPV was no surprise. As was noted earlier in this study, per the DAU acquisition guidelines, open source software alternatives should be considered when acquiring a solution. It is important to note that all the WSUS-based tools were significantly cheaper than their CM counterparts. Thus, Local Update Publisher won first place in the CBA among non-CM tools. As depicted in Table 10, the NPV of LUP was $713,930.

The second place alternative recommended by the CBA is SolarWinds Patch Manager, again illustrated in Table 10, with a positive NPV of $661,795. The third place alternative recommended is eEye Retina CS, with a positive NPV of $397,393. The fourth place alternative recommended is LANDesk LDMS, with an NPV of negative $214,589. For the remainder of the alternatives, please refer to Table 10.

It should be noted that if the cost of remediating the damages inflicted by a single cyber attack was adjusted from the $24,000 figure used in this analysis to a much larger

number, such as the $234,244 figure cited by the 2009 Computer Crime and Security Survey, then all the tools will generate a positive NPV, ROI and IRR.[238]

NPV, ROI, IRR	LUP	SolarWinds PM	Retina CS	LANDesk LDMS	MS SCCM 2012	IBM TEM	HP HPCA	ALTIRIS CMS	CFEngine
NPV*	**$713,930**	**$661,795**	**$397,393**	**-$214,589**	-$265,189	-$489,856	-$667,966	-$926,411	-$3,051,672
ROI	0.0%	1225.8%	120.9%	-22.2%	-26.1%	-38.6%	-46.3%	-54.6%	-76.0%
IRR	0.0%	1198.9%	148.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

* assumes a 3.3% discount rate

Table 10. NPV, ROI, IRR of Alternatives Assuming a Cost of $24,000 per Incident for Remediation

Table 11 shows the NPV, ROI and IRR results assuming a per incident cost of $234,244. The individual rankings between each tool did not change; however, the NPV differences between the tools shrank drastically. The NPV percentage difference between LUP and Retina CS shrank to only 4.8 percent. When using the $24,000 per incident number, the percentage difference was 79.6 percent. Even the tool with the lowest NPV in the CBA, CFEngine 3, still generated a positive NPV of $3,202,472 when the higher per incident cost was used. While the differences between NPV shrank substantially among the tools, the differences in ROI and IRR generated by each tool remained very significant. Despite this, at $234,244 per incident for remediation costs, every single tool in the analysis looks like an amazing investment, with even CFEngine 3 having an ROI of 79.8 percent. The fact is that the individual cost to remediate a cyber attack varies tremendously depending on numerous factors. As the cost of remediation increases, the relative importance attached to the cost of a third-party remediation tool decreases.

[238] Richardson, "2009 Computer Crime and Security Survey," 2; Pisello, "Is There a Business Case for IT Security?" 10.

NPV, ROI, IRR	LUP	SolarWinds PM	Retina CS	LANDesk LDMS	MS SCCM 2012	IBM TEM	HP HPCA	ALTIRIS CMS	CFEngine
NPV*	**$6,968,074**	**$6,915,939**	**$6,651,537**	**$6,039,555**	$5,988,955	$5,764,288	$5,586,178	$5,327,732	$3,202,472
ROI	0.0%	12809.4%	2023.1%	623.9%	589.1%	453.9%	387.5%	314.0%	79.8%
IRR	0.0%	12240.0%	2099.9%	735.7%	558.7%	795.8%	468.4%	316.7%	303.6%

* assumes a 3.3% discount rate

Table 11. NPV, ROI, IRR of Alternatives Assuming a Cost of $234,244 per Incident for Remediation

V. CONCLUSION/RECOMMENDATIONS

A. CONCLUSION

It is obvious from the analysis in Chapter IV that no tool was able to meet all the requirements of an optimal third-party vulnerability management tool. In the words of the French philosopher Voltaire, "perfect is the enemy of the good." Voltaire meant that as good nears perfection, it becomes ever more difficult to achieve.[239] Too often the U.S. Army, as well as the DoD, have tried to chase perfection when fielding new equipment or capabilities. The predictable result is that new equipment and capabilities often take years to field; in other words, they are either already obsolete or nearing obsolescence by the time they are deployed. Now that the Army has deployed SCCM 2007 to the majority of the NIPRNET, Microsoft has released SCCM 2012, which will require yet another resource intensive, time consuming deployment. The decision to use COTS software was, in part, meant to address this problem. However, COTS solutions do not always address the complexity and resulting enterprise-wide deployment problems that often result from adopting IT tools like SCCM 2007. No matter how capable a tool is, its value is drastically diminished if it cannot be rapidly fielded. General George S. Patton said it best, "a good plan violently executed now is better than a perfect plan next week."[240] In this case, not only does the Army need an effective tool for patching third-party vulnerabilities, it needs a tool that can be deployed enterprise-wide in a matter of months, not years.

Table 12 reflects the priority one requirements identified in the requirements analysis. Only eEye Retina CS was capable of meeting every top priority requirement. SolarWinds PM only trailed Retina CS because it lacked Retina NSS integration. LUP met most of the top requirements, but its steep learning curve, poor integration with the WSUS console, and uncertain future development, were major detractors. All the full featured CM tools lacked the capability to support the Army or the DoD with a single

[239] Wikiquote, "Voltaire," http://en.wikiquote.org/wiki/Voltaire.

[240] Michael Moncur, "The Quotations Page," 2012, http://www.quotationspage.com/quote/34219.html.

hierarchy. A steep learning curve, a high degree of deployment difficulty and lack of integration with Retina NSS hurt nearly all the full featured CM tools. SCCM 2012, Altiris CMS and LDMS all achieved identical scores when evaluating priority one requirements. IBM Tivoli deserves credit for its massive single core server scalability and the ease with which it can be deployed to support a widely dispersed network. Of the full feature CM tools, only CFEngine 3, which is primarily a management tool for Linux clients, and HP Client Automation, really miss the mark. HPCA misses the mark because it does not automatically deploy third-party updates. The main problem with CFEngine 3 lies in the fact that administrators would have to learn a new programming language, which would be a significant barrier to adoption.

PRIORITY ONE REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Single Hierarchy Scalable to Army?	1							✓	✓	✓
Tiered Architecture?	1	✓	✓	✓		✓	✓	✓	✓	✓
Create and Distribute Patches at Top Tier?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Child Servers Can Replicate Patch Content and Approvals From Parents?	1	✓	✓	✓		✓	✓	✓	✓	✓
Child Servers Can Operate Autonomously From Parent?	1	✓	✓	✓				✓	✓	✓
Average NOSC Admin Capable of Deployment and Configuration?	1				✓	✓		✓	✓	✓
Requires Less Than Eight hrs Formal Training and Less Than Three Days OJT for Basic Tool Operation?	1							✓	✓	
Automated Third-Party Patch Deployment For Designated Collections?	1	✓	✓	✓	✓		✓	✓	✓	✓
Built-in Detection Logic?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Uses Certificate Based Authentication (PKI)?	1	✓	✓	✓	✓	✓		✓	✓	✓
Supports Role Based Assignment of Admin Permissions?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integration With eEye Retina NSS?	1								✓	
Can Function Properly on Unstable Networks With Low Bandwidth?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supports Bandwidth Control?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Meets FIPS 140-2?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Meets CCEVS?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Capable of Meeting Army CON Requirements?	1	✓	✓	✓	✓	✓	✓	✓	✓	✓
Vendor Has Support Plan for Tool?	1	✓	✓	✓	✓	✓	✓	✓	✓	

Table 12. Priority One Requirements

Table 13 depicts each of the priority two requirements. Retina CS met more of these requirements than any other tool, although it was trailed closely by LDMS. Most of

the tools possessed similar core functionality, such as a GUI-based console, reliance on a client agent, the capability to be hosted on a VM server, support for Windows Server and SQL Server 2008, interaction with MS AD, client device grouping, compliance with AR 25-2 security measures and rollup reporting. A key differentiator between the tools was their ability to scale to the DoD level with only a single hierarchy. Again, only the WSUS-based tools have the potential to accomplish this scalability. Another major difference between tools was patching support for Mac, Unix, and Linux devices, which only Altiris CMS, LANDesk LDMS, IBM TEM and CFEngine are capable of providing, without a third-party add-on. Interestingly, only half the tools supported a web-based console. Tools, such as SCCM, SolarWinds PM, IBM TEM and LUP, all require a standalone console installation to manage the tool remotely, which is an annoyance. With the increasing importance of mobile device management, it is surprising that none of the tools has the capability to patch these devices, although IBM TEM can deploy apps to iOS and Android devices. Most of the tools have some form of MDM, but capabilities are mostly limited to monitoring functions. As the importance of MDM increases, CM tools should being to incorporate additional management and remediation functionality over mobile devices.

PRIORITY TWO REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Single Hierarchy Scalable to DoD?	2							✓	✓	✓
Tool Can be Hosted by a VM Server?	2	✓		✓	✓		✓	✓	✓	✓
Highly Detailed Documentation?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
GUI Based Console?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Control Tool From Web Browser?	2		✓	✓		✓	✓		✓	
Supports MS Server 2008 and SQL Server 2008?	2	✓	✓	✓	✓	✓		✓	✓	✓
Uses Client Agent?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Patches Mac, Unix, Linux?	2		✓	✓	✓		✓			
Update Mobile Devices: Android, iOS, Blackberry?	2									
Interfaces with MS AD?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Automated Repair of Misbehaving Agents?	2			✓				✓		
Prevent User from Cancelling Patch Install?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Supports Client Grouping by Type, OS, and Functional Designation?	2	✓	✓	✓	✓	✓		✓	✓	✓
Generate IAVM Compliance Reports?	2					✓			✓	
Report Rollups Avaiable at Top Tier?	2	✓	✓	✓	✓	✓	✓	✓	✓	✓
Could Potentially Provide a DoD-Wide Third-Party Patching Solution?	2							✓	✓	✓
Tracks Logon Attempts?	2	✓	✓	✓	✓	✓	✓	✓	✓	
Maintains User Logon Data?	2	✓	✓	✓	✓	✓	✓	✓	✓	
Cost Competitive With Market Leaders?	2	✓		✓				✓	✓	✓
Cost Less Than Current Solution?	2			✓				✓	✓	✓

Table 13. Priority Two Requirements

Table 14 reflects the priority three requirements. Microsoft SCCM met all but one of the requirements, which was updating networking devices, which no tool in the analysis was capable of meeting. LANDesk LDMS and IBM TEM each came up short on two requirements, while Altiris CMS failed to meet three. The remaining tools each failed to meet at least four requirements. Considering that priority three requirements fall under the "nice to have, but not essential" group, this deficiency is not considered a serious detractor to the tools' capabilities.

PRIORITY THREE REQUIREMENTS	Priority	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
10-Minute Tutorial Video?	3	✓		✓			✓	✓	✓	
CLI Console Support?	3	✓	✓	✓	✓	✓	✓	✓	✓	✓
Update Networking Devices?	3									
Quarantine Out of Compliance Clients?	3	✓			✓					
Agent Deployment Using AD Group Policy?	3	✓	✓	✓	✓	✓		✓	✓	✓
Agent Check-In Frequency Adjustable?	3	✓	✓	✓	✓	✓	✓		✓	
Allow User to Delay Patch Installation?	3	✓	✓	✓	✓					

Table 14. Priority Three Requirements

FM 5-0, *The Operations Process*, suggests using a decision matrix to aid in selecting the best COA.[241] Table 15 presents the decision matrix used to make final recommendations on each of the tools. Support for priority one requirements are considered mandatory and are assessed a high value of 10-points each. Priority two requirements are worth four points each and are considered very important features. Priority three requirements were assessed a value of two points and represent the least important requirements. This scoring is highly subjective, and it would be possible to change the point values to favor one tool over another. In addition, not all priority one or two requirements have the same value relative to each other. Still, applying a subjective standard scoring level to each requirement is a useful way to see how the tools compared with each other. Since the analysis in Chapter IV placed a high degree of importance on scalability, as well as ease of use and deployment, both Retina CS and SolarWinds PM scored higher than the full featured CM tools in this analysis, despite having fewer features.

[241] Headquarters, Department of the Army, *FM 3-13, The Operations Process* (Washington, DC: U.S. Army Training and Doctrine Command), March 2010, https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fm5_0.pdf?&client_name=ARMYPUBS&CAC=CAC+Login, B-35.

DECISION MATRIX	Weight	MS SCCM 2012	ALTIRIS CMS	LANDesk LDMS	IBM TEM	HP HPCA	CFEngine	SolarWinds PM	Retina CS	LUP
Priority 1 *(18 Requirements)*	10 Pts	14	14	14	12	13	12	17	18	15
Priority 2 *(20 Requirements)*	4 Pts	12	12	16	12	12	11	16	17	13
Priority 3 *(7 Requirements)*	2 Pts	6	4	5	5	3	3	3	4	2
Adjusted Score*		**194**	**192**	**209**	**173**	**181**	**167**	**237**	**252**	**204**

Table 15. Tool Decision Matrix

Taking into account the results of the CBA, eEye Retina CS comes closest to meeting U.S. Army's requirements for an optimal third-party patching solution. However, it has several shortcomings, the most significant of which is a lack of support for Mac, Linux and Unix devices. Still, it possesses the scalability potentially to meet DoD and U.S. Army requirements using only a single hierarchy. It is reasonably easy to deploy and it is simple to operate. Its most significant advantage over every other tool analyzed was its integration with Retina NSS. This capability allows Retina CS to resolve one of the greatest challenges faced by the current IAVM process, which is a lack of interaction between the patching tool and the network security scanner used by IA. Another bonus of Retina CS is its native MDM capabilities for Blackberry, Android and ActiveSync managed devices. The end result is that Retina CS has the greatest capability set of the WSUS-based tools. As a result of this analysis, the Retina CS tool came the closest to meeting U.S. Army requirements for an ideal third-party patching tool.

SolarWinds Patch Manager came in very close to Retina CS in final scoring. It holds the same scalability and deployment advantages and is arguably the best tool in the usability realm due to its consoles similarity to the WSUS console. However, it has essentially the same shortcomings as Retina CS, which includes support for only Windows devices. Unlike Retina CS, it has no MDM support and no integrated scanner. It does, however, represent the best value in the analysis by a wide margin. If low cost

was the primary decision-making factor, SolarWinds PM would be the logical fiscal choice.

Despite meeting many of the most significant requirements and finishing first in the CBA, LUP is not an acceptable third-party patching solution in its present state. It is much more work intensive than both Retina CS and SolarWinds PM to create and deploy third-party patches. The most significant problem with LUP is that it requires the use of an entirely separate console, in addition to the standard WSUS console, for managing third-party patches. If this tool allowed third-party patches to be visible in the WSUS console, it would have been a viable alternative, especially as an open source tool.

LANDesk LDMS finished at the top of the full featured CM solutions and third overall in the analysis, but like all other CM solutions in this analysis, LDMS is incapable of supporting the DoD or U.S. Army with a single hierarchy. LDMS finished ahead of SCCM 2012 because of its additional feature set and slightly higher NPV. While LDMS does not have the scalability of SCCM 2012, it does have native automated patching support for Mac, Linux, and Unix devices, the ability to repair misbehaving clients, a web-based console, while SCCM fails to meet these requirements. Still, SCCM 2012 does have several advantages over the other full featured CM tools in this comparison. The first advantage is scalability, which at 400,000 clients per hierarchy, is the best of the full featured CM tools. Second, the Army has several years of experience with SCCM 2007 and has learned to use if effectively. This experience should greatly aid in the deployment and effectiveness of SCCM 2012, as the tool is fundamentally similar to the 2007 version. Third, SCCM 2012 has a vast amount of third-party add-on module support; more than any other tool in this analysis, which provides SCCM with unmatched expandability, but at an additional cost. Fourth, SCCM has a large installed base, with a very active user community and reliable support from Microsoft. Symantec CMS finished just behind SCCM. It is held back by its relatively poor scalability of 100,000 clients per hierarchy and the fact that it cannot be hosted by a virtual server. Still, Symantec CMS does provide native patching support for Mac, Linux, and Unix devices.

HP HPCA also finished closely behind SCCM and Symantec CMS, but despite its score, HPCA did not meet the critical requirement of automated deployment of third-

party updates. HPCA was the only tool that lacked this capability. IBM TEM was held back by its lack of hierarchy support and use of the proprietary *fixlet* language for authoring client policies. Its most outstanding feature is its tremendous capacity from an extremely small server footprint. A single core server, with associated database, supports up to 250,000 clients. As a result of its simple architecture, IBM TEM is easier to deploy than every other full featured CM solution in this analysis. Still, TEM's lack of hierarchy support prevented it from scaling to support the needs of the DoD and U.S. Army with a single hierarchy. CFEngine 3 finished with the lowest overall score in this analysis. Its high complexity combined with an NPV worse than its competitors were significant drawbacks. If the Army's client environment was primarily Mac, Unix, or Linux based, this tool would be an excellent choice.

B. RECOMMENDATIONS FOR THE U.S. ARMY

It is the recommendation of the authors that the U.S. Army adopt eEye Retina CS as the enterprise standard NetOps tool for mitigating third-party application vulnerabilities. Given the Army's plans to transition from SCCM 2007 to SCCM 2012, this recommendation is unlikely to be taken. Value exists, however, in deploying Retina CS in parallel with SCCM and would provide several benefits. The first benefit is that third-party patch creation could be nullified because Retina CS includes an extensive third-party patch subscription service that would drastically reduce the burden of patch content creation, which is currently performed by the NETCOM G5. The second benefit is integration with Retina NSS, which is a capability that SCCM lacks. This integration allows NOSC or TNOSC administrators to scan and remediate information systems using only Retina CS, along with its scanning agent, Retina NSS, and potentially eliminating the problem of false positives with which the Army continues to struggle. Third, Retina CS could be easily deployed to Army organizations currently untouched by Microsoft SCCM. Given the ease with which Retina CS can be deployed and operated, nearly any Army organization should be capable of putting Retina CS into operation and patching its information systems within a matter of days. Many Army units may find that they prefer using Retina CS over SCCM, especially NOSCs and tactical organizations at the division or BCT level. Due to the ease of use that Retina CS brings to the table, it is highly likely

that these units will make more effective use of Retina CS in comparison to SCCM, although TNOSCs are still likely to prefer SCCM, given its greater capability set.

Should funding be at a level that does not support the acquisition of Retina CS, the next best alternative is SolarWinds Patch Manager. SolarWinds PM provides all of the third-party patching capability that Retina CS does, but without the benefits of integrating with Retina NSS. With an NPV nearly twice that of Retina CS and an ROI nearly ten times that of Retina CS, SolarWinds PM represents a fantastic value. Like Retina CS, ease of use and deployment are strong points of SolarWinds PM. Current WSUS administrators will immediately feel comfortable using this tool.

LANDesk LDMS came the closest of the full featured CM tools to meeting the requirements identified in this analysis. It also had the best NPV of the full featured CM tools at negative $214,589 when using $24,000 as the per incident cost of a cyber attack, which makes it the best alternative for the U.S. Army if NETCOM leadership is only willing to accept a full featured CM solution to handle third-party vulnerability management. If this option is chosen, the Army should consider increasing system administrator manning at the NOC/NOSC and BCT levels because LDMS is a complex tool that really should be assigned a subject matter expert dedicated to the tools operation. By increasing manning, the Army could potentially allow for one soldier to be dedicated to the operation of LDMS at each NOSC/BCT.

SCCM 2012 is the authors' second place recommendation among the full featured CM tools. Certainly, a good argument can be made for keeping Microsoft SCCM, based on an established infrastructure, years of Army experience with the SCCM, expandability and the popularity of the tool. These factors are all significant, but the fact remains that LDMS is a more capable tool than SCCM and has a slightly better NPV.

C. SUGGESTIONS FOR FUTURE WORK

The authors chose to address the problem of third-party application vulnerabilities from an Army centric position. In reality, this problem is DoD wide. The DoD as a whole is in need of an effective, unified third-party vulnerability management solution that most

likely has requirements very similar to those presented for the U.S. Army in this analysis. Future research should address this larger problem.

A significant limitation of this thesis was that the authors did not conduct large-scale field tests of each of the available vulnerability management solutions. Large-scale experimentation would be useful in discovering potential problem areas that cannot be determined from conducting secondary research combined with limited virtual laboratory testing. Conducting large-scale testing, on the order of at least 10,000 client devices per tool, could also provide answers to the performance requirements, which were left unanswered by this study. Testing of this magnitude is difficult to achieve, even for organizations as large as the U.S. Army. The authors recommend that an entirely virtual environment be constructed to reduce the costs associated with conducting large-scale testing.

Another area in which additional research is needed is determining the average cost incurred by the U.S. Army for a single successful cyber attack. This data could potentially be obtained from each of the Regional Computer Emergency Reponses Teams (RCERT) typically collocated with each TNOSC, which should provide a more accurate measure of the costs incurred by the U.S. Army for an average cyber attack, and lead to a more accurate CBA.

LIST OF REFERENCES

Andress, Mandy. “Windows Patch Management Tools.” *Network World*. 2003. http://books.google.com/books?id=YxkEAAAAMBAJ&pg=PT37&dq=microsoft+sus+released&hl=en&sa=X&ei=CdFGT-e8O-bSiAL42ITbDQ&sqi=2#v=onepage&q=microsoft%20sus%20released&f=false.

Army CIO G6. “Common Operating Environment Architecture: Appendix C to Guidance for ‘End State’ Army Enterprise Network Architecture.” October 1, 2010. http://ciog6.army.mil/LinkClick.aspx?fileticket=udbujAHXmK0%3D&tabid=79.

———. “Global Network Enterprise Construct Implementation Plan.” *Army Chief Information Officer G-6*. November 2010. http://ciog6.army.mil/LinkClick.aspx?fileticket=3MWHY5M9nHQ%3D&tabid=100.

Army Cyber Command. “2012-A-0029 Multiple Vulnerabilities in Adobe Flash Player.” February 2012.

Army Reserve. “335th Signal Command Theater.” (n.d.). http://www.usar.army.mil/arweb/organization/commandstructure/USARC/OPS/335Sig/Pages/default.aspx.

Ash, Tim, and Mike Spragg. “NetOps Implementation Update (CMDB, SMS/MOM, SCTS.).” *U.S. Army Network Enterprise Technology Command*. August 22, 2007. www.afcea.org/events/pastevents/documents/Track4Session5-NetOpsUpdate.ppt.

Baker, Wade H., David C. Hylender, and Andrew J. Valentine. “2008 Data Breach Investigations Report.” *Verizon Business Risk Team.* 2008. http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

Barnette, Mark and Adelia Wardle. “Microsoft Enterprise License Agreement.” *Program Executive Office Enterprise Information Systems*. February 11, 2004. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CC0QFjAB&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2Fc%2F3%2Fe%2Fc3e4206c-931c-4746-a1ed-52f0d19dc5ba%2FWardleBarnette_ArmySymp2004.ppt&ei=4zScT73-FoGliQLK5ux9&usg=AFQjCNHMRmuZf4lk8fMsRm5x-6fOO49q-Q&sig2=65pSNWjyUHnPgMfDGx1JlA.

Bellissimo, Anthony, John Burgess, and Kevin Fu. “Secure Software Updates: Disappointments and New Challenges.” Proceedings of the 1st USENIX Workshop on Hot Topics in Security. *USENIX Association*. 2006. http://static.usenix.org/event/hotsec06/tech/full_papers/bellissimo/bellissimo.pdf.

Bit 9. “Web Browsers, Desktop Software Top Dirty Dozen Apps List.” 2010. http://www.bit9.com/company/news-release-details.php?id=175.

Blanchard, Benjamin S. *System Engineering Management*. 4th ed. New Jersey: John Wiley and Sons, 2008.

Boardman, Anthony, David Weimer, Aidan R. Vining, and David Greenberg. *Cost-Benefit Analysis: Concepts and Practice.* 3rd ed. New Jersey: Prentice Hall, 2005.

Bowens, Roland. “Fort Rucker, Fort Monroe Etch an NEC Success Story.” *Army Communicator*. Fall 2010. http://findarticles.com/p/articles/mi_m0PAA/is_3_35/ai_n56745408/.

Brandel, Mary. “How to Compare Patch Management Software.” *CSO Online*. 2009. http://www.csoonline.com/article/507070/how-to-compare-patch-management-software?page=4.

Brock, Jerome P. “CSSAMO Experiences in Operation Iraqi Freedom.” *Army Logistician*. 2007. http://www.almc.army.mil/alog/issues/JanFeb07/cssamo_exper.html.

Broussard, Frederick W., Randy Perry, and Tim Grieser. “Gaining Business Value and ROI with LANDesk Software: Automated Change and Configuration Management.” *IDC.* January 2011. http://www.creekpointe.com/landesk/pdf/IDCBusinessValue.pdf.

Carden, Michael J. “Cyber Task Force Passes Mission to Cyber Command.” *American Forces Press Service*. September 8, 2010. http://www.af.mil/news/story.asp?id=123221046.

CBS Interactive Staff. “DoD Gates: We’re always under cyberattack.” *ZDNet*. April 22, 2009. http://www.zdnet.com/news/dod-gates-were-always-under-cyberattack/290770.

CERT. “2010 Cyber Security Watch Survey: Cybercrime Increasing Faster Than Some Company Defenses.” January 25, 2010. http://www.cert.org/archive/pdf/ecrimesummary10.pdf.

CFEngine. “CFEngine @ Work: Worldwide Customer Success.” 2012. https://cfengine.com/use_cases.

———. “CFEngine Quick Start Guide.” 2012. https://cfengine.com/manuals/cf3-quickstart#!prettyPhoto[gal1]/1/.

Chertoff, Michael, Mike McConnel, and William Lynn. “China’s Cyber Thievery is National Policy-and Must Be Challenged.” *Wall Street Journal*. January 27, 2012. http://online.wsj.com/article/SB10001424052970203718504577178832338032176.html.

CIO. “8 Elements of Complete Vulnerability Management.” *Chief Information Officer Online*. October 2009. http://www.cio.com/documents/whitepapers/VulnerabilityManagement.pdf.

Colley, Andrew. “Symantec Australia to Shutter Software Unit.” *The Australian*. June 8, 2011. http://www.theaustralian.com.au/australian-it/symantec-australia-to-shutter-software-unit/story-e6frgakx-1226071891896.

Colville, Ronni J., and Michael A. Silver. *Magic Quadrant for PC Life Cycle Configuration Management 2005*. (Gartner RAS Core Research Note G00131185), 2005.

Connor, Alice. *U.S. Army Cyber Command Execute Order (EXORD) 2011-090 Implementation and Integration of System Center Configuration Management (SCCM) and NIPRNET and SIPRNET.* U.S. Army Cyber Command, Fort Belvoir, VA, September 20, 2011.

Cosgrove, Terrence. *Magic Quadrant for PC Configuration Life Cycle Management Tools.* Gartner Inc., November 24, 2009.

———. *Magic Quadrant for Client Management Tools*. Gartner Inc. January 31, 2012.

Czumak III, Michael. “Recommendations for a Standardized Program Management Office (PMO) Time Compliance Network Order (TCNO) Patching Process.” Master’s thesis, Air Force Institute of Technology, 2007.

Defense Acquisition University. *Systems Engineering Fundamentals.* Fort Belvoir, VA. 2001. http://www.dau.mil/pubs/pdf/SEFGuide%2001-01.pdf.

Defense Information Systems Agency. “Termination of Secure Configuration Remediation Initiative (SCRI) Support.” September, 2010. http://iase.disa.mil/tools/disa_termination_of_scri_support.doc.

Delaet, Thomas, Wouter Joosen, and Bart Vanbrabant. “A Survey of System Configuration Tools.” Proceedings of the 24th Large Installations Systems Administration (LISA) conference, *USENIX Association*. San Jose, CA, November 2010.

Department of Defense. “Department of Defense Strategy for Operating in Cyberspace.” July 2011. http://www.defense.gov/news/d20110714cyber.pdf.

Dixon, David. “SCCM\WSUS—Streaming From an Upstream Server.” *Microsoft TechNet.* May 14, 2009. http://blogs.technet.com/b/daviddixon/archive/2009/05/14/sccm-wsus-streaming-from-an-upstream-server.aspx.

Duebendorfer, Thomas, and Steven Frei. *Why Silent Updates Boost Security*. Technical Report 302. TIK, ETH Zurich. 2009. http://www.techzoom.net/silent-updates.

eEye Digital Security. “Retina CS Add-On: Patch Management Module.” 2012. http://www.eeye.com/eEyeDigitalSecurity/media/Datasheets/Retina%20CS%20Add-Ons/Retina-CS-Patch-Mgmt-DS.pdf.

———. “Retina CS Management Console.” 2012. http://www.eeye.com/eEyeDigitalSecurity/media/Datasheets/Retina/Retina-CS-DS.pdf.

———. “Retina CS, Retina Insight Solution Briefing.” 2011. http://www.youtube.com/watch?v=egWcwYYidxg&feature=relmfu.

Eisenberger, I., and G. Lorden. *Life-Cycle Costing: Practical Considerations*. DSN Progress Report 42-40, May and June, 1977.

Elaine, Shannon. “The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them).” *Time Magazine*. August 29, 2005. http://www.time.com/time/magazine/article/0,9171,1098961,00.html.

Emerson Network Power. “Understanding the Cost of Data Center Downtime: An Analysis of the Financial Impact on Infrastructure Vulnerability.” 2011. http://emersonnetworkpower.com/en-US/Brands/Liebert/Documents/White%20Papers/data-center-uptime_24661-R05-11.pdf.

EminentWare. “Deploy and Manage 3rd Party Patches and Applications.” http://www.eminentware.com/assets/pdfs/EminentWare-WSUS-Extension-Pack-005-Datasheet2.pdf.

———. “EminentWare WSUS Extension Pack and Microsoft System Center Configuration Manager.” 2009. https://www.eminentware.com/cs2008/media/p/277.aspx.

Ezzat, Meged. “What’s New in Configuration Manager 2012 “SCCM 2012”—Part 1—“Overview.” *Microsoft TechNet*. August 10, 2011. http://blogs.technet.com/b/meamcs/archive/2011/08/10/what-s-new-in-configuration-manager-2012-sccm-2012.aspx.

Faust, Joseph. “Reducing Organizational Risk through Virtual Patching.” *SANS Institute*. 2010. http://www.sans.org/reading_room/whitepapers/application/reducing-organizational-risk-virtual-patching_33589.

Floyd, Elizabeth, Benita Vailoff, and Tom Stuckey. “IT Asset Management: Information Exchange Forum Session: 2.” Proceedings from the LandWarNet Conference. *Armed Forces Communications and Electronics Association.* April 2011. http://www.afcea.org/events/pastevents/documents/LWN11_ITAM_Session_2.pdf.

G3 7th SC (T). “7th Signal Command Theater: One Team One Network.” *Armed Forces Communications and Electronics Association.* September 30, 2009. http://www.afcea-augusta.org/industry_day_slides/day1/7th_Sig_Industry_Day_Brief_(releasable).pdf.

Gerace, Thomas, and Huseyin Cavusoglu. “The Critical Elements of the Patch Management Process.” *Communications of the ACM* 52, no. 8 (August 2009). http://doi.acm.org/10.1145/1536616.1536646.

Gkantsidis, Christos, Thomas Karagiannis, Pablo Rodriguez, and Milan Vojnović. “Planet Scale Software Updates.” Proceedings of SIGCOMM. *ACM SIGCOMM*. September 11–15, 2006. http://www.cs.ucr.edu/~tkarag/papers/planet_scale_updates.pdf.

Gordon, Lawrence A., and Martin Loeb. *The Economics of Information Security Investment*. ACM. 2002.

Hagenus, Scott. “Security Vendors Can no Longer Ignore Patch Management.” *SC Magazine*. February 3, 2012. http://www.scmagazine.com/security-vendors-can-no-longer-ignore-patch-management/article/226232/.

Headquarters, Department of the Army. *AR 25-1, Army Knowledge Management and Information Technology*. Washington, DC: U.S. Army Training and Doctrine Command. 2008. http://armypubs.army.mil/epubs/pdf/r25_1.pdf.

———. *AR 25-2, Information Assurance*. Washington, DC: U.S. Army Training and Doctrine Command. 2009. http://armypubs.army.mil/epubs/pdf/r25_2.pdf.

———. *FM 3-13, The Operations Process.* Washington, DC: U.S. Army Training and Doctrine Command. March 2010. https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fm5_0.pdf?&client_name=ARMYPUBS&CAC=CAC+Login.

———. *FM 5-0, Information Operations: Doctrine, Tactics, Techniques, and Procedures.* Washington, DC: U.S. Army Training and Doctrine Command. 2003. https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fm3_13.pdf.

———. *FM 6-02.60, Tactics Techniques and Procedures (TTPs) for the Joint Network Node—Network (JNN-N).* Washington, DC: U.S. Army Training and Doctrine Command. 2006. https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fmi6_02x60.pdf.

HP. "HP Client Automation Enterprise Edition for the Windows Operating System 8.10: Getting Started Guide." *Hewlett-Packard Development Company, L.P*. February 2012. http://support.openview.hp.com/selfsolve/document/KM1332107/binary/CA8.10_CoreSat_GSG_Concepts.pdf?searchIdentifier=267d8d34%3a136a77065e3%3a476e&resultType=document.

———. "HP Client Automation Enterprise Patch Management for Windows and Linux Operating Systems 8.10." *Hewlett-Packard Development Company, L.P.* February 2012. http://support.openview.hp.com/selfsolve/document/KM1332147/binary/CA8.10_PatchMgt_RG.pdf?searchIdentifier=267d8d34%3a136a77065e3%3a462d&resultType=document.

———. "HPCA Platform Support Matrix." *Hewlett-Packard Development Company, L.P.* November 11, 2011. http://support.openview.hp.com/selfsolve/document/KM1332718/binary/CA8.10_Support_Matrix.pdf?searchIdentifier=32ae5388%3a1370f5188b2%3a-710a&resultType=document.

IBM. "Selecting the Right Solution for Endpoint Management." *IBM Software*. January 2012. http://public.dhe.ibm.com/common/ssi/ecm/en/tio14008usen/TIO14008USEN.PDF.

———. "Tivoli Endpoint Manager: Mobile Device Management." *IBM Software.* April 3, 2012. https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Endpoint%20Manager/page/Mobile%20Devices%20Overview.

Joint Task Force. "Recommended Security Controls for Federal Information Systems and Organizations." National Institute of Standards and Technology. NIST Special Publication 800–53. Gaithersburg, MD, August 2009.

Keizer, Gregg. "Researchers Unearth More Chinese Links to Defense Contractor Attacks." *Computerworld*. January 27, 2012. http://www.computerworld.com/s/article/9223765/Researchers_unearth_more_Chinese_links_to_defense_contractor_attacks.

Kruse, Peter. "This is How Windows Gets Infected with Malware." *CSIS Security Group*. September 27, 2011. http://www.csis.dk/en/csis/news/3321/.

LANDesk. “LANDesk Management Suite 9.0 Configuration the LANDesk Management Suite/ALM Patch Integration.” *LANDesk Software Inc.* 2009. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CEoQFjAC&url=http%3A%2F%2Fcommunity.landesk.com%2Fsupport%2Fservlet%2FJiveServlet%2Fdownload%2F5098-5-22975%2FLDMSPatchProcessIntegration90.pdf&ei=D2SDT531HKiQiQKQjtHjBQ&usg=AFQjCNFCFNS54kRuudMPFkgTz2xElKIJOQ&sig2=AFxJRukQ3l8pPVmwTfQxOg.

———. “LANDesk Management Suite 9.0 Core Synchronization.” *LANDesk Software Inc*. 2012. http://help.landesk.com/Topic/Index/ENU/LDMS/9.0/Content/Windows/sync_o_overview.htm.

———. “LANDesk Management Suite 9.0 User’s Guide.” *LANDesk Software Inc.* 2011. http://www.landesk.com/resources/product-documentation.aspx#ldms90.

Liebowitz, Matt. “Chinese Sykipot Malware Targets U.S. Government.” *MSNBC*. January 13, 2012. http://www.msnbc.msn.com/id/45985897/ns/technology_and_science-security/t/chinese-sykipot-malware-targets-us-government/#.TzBSiaX2aHw.

Litty, Lionel, and David Lie. *Patch Auditing in Infrastructure as a Service Clouds.* New York, NY: ACM, 2011.

Local Update Publisher. “Local Update Publisher: Publish Your Own Updates to WSUS.” 2010. http://localupdatepubl.sourceforge.net/index.html.

Massey, H.G., David Novick, and R.E. Peterson. *Cost Measurement: Tools and Methodology for Cost Effectiveness Analysis.* The RAND Corporation. Santa Monica, CA, February 1972.

McDowell, Mindi. “Cyber Security Tip ST06-001: Understanding Hidden Threats: Rootkits and Botnets.” *US-Cert*. August 26, 2011. http://www.us-cert.gov/cas/tips/ST06-001.html.

Mell, Peter, and Miles C. Tracy. *Procedures for Handling Security Patches*. National Institute of Standards and Technology. NIST Special Publication 800–40. Gaithersburg, MD, April 2002.

Mell, Peter, Tiffany Bergeron, and David Henning. *Creating a Patch and Vulnerability Management Program: Recommendations of the National Institute of Standards and Technology (NIST).* Special Publication 800–40, Gaithersburg, MD, 2005. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

Microsoft. “About System Center Update Publisher.” *Microsoft TechNet*. 2012. http://technet.microsoft.com/en-us/library/bb632895.aspx.

———. “End to End Service Monitoring With Microsoft System Center Operations Manager 2007.” *Microsoft TechNet*. 2007. http://technet.microsoft.com/en-us/systemcenter/om/bb498233.

———. “Local Publishing.” (n.d.). http://msdn.microsoft.com/en-us/library/bb902470.

———. “Supported Configurations for Configuration Manager.” *Microsoft TechNet*. 2012. http://technet.microsoft.com/en-us/library/gg682077.aspx#BKMK_SupConfigSystemReqs.

———. “System Center Configuration Manager Overview.” *Microsoft*. August 2011. http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-overview.aspx.

———. “Systems Management Server.” *Microsoft TechNet*. (n.d.). http://technet.microsoft.com/en-us/library/cc723685.aspx.

———. “Third-Party Custom Catalogs for Configuration Manager 2007 and System Center Essentials 2007.” 2012. *Microsoft TechNet*. http://technet.microsoft.com/en-us/systemcenter/cm/bb892875.aspx.

———. *Performance Work Statement For United States Army Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM/9th SC (A)), Enterprise Systems Technology Activity (ETSA) For Microsoft Consulting Services For Systems Management (SysMan) Sustainment Support*, Microsoft, July 13, 2009.

Mills, Elinor. “Pentagon Spends Over $100 million on Cyberattack Cleanup.” *CNET News*. April 7, 2009. http://news.cnet.com/8301-1009_3-10214416-83.html.

Mitre. “About CVE Identifiers.” *National Cyber Division of the U.S. Department of Homeland Security*. January 10, 2012. http://cve.mitre.org/cve/identifiers/index.html.

Monahan, Susan. “GNE SysMan Updates.” Proceedings from the LandWarNet Conference. *Armed Forces Communications and Electronics Organization*. Tampa, FL, April 23, 2011.

Moncur, Michael. “The Quotations Page.” *The Quotations Page*. 2012. http://www.quotationspage.com/quote/34219.html.

Montalbano, Elizabeth. “DOD Approves Dell Android Tablet for Use.” *InformationWeek Government*. October 31, 2011. http://www.informationweek.com/news/government/mobile/231901988.

National Information Assurance Partnership. “Validated Products List.” 2012. http://www.niap-ccevs.org/vpl/.

National Institute of Standards and Technology. “Recommended Security Controls for Federal Information Systems and Organizations: NIST Special Publication 800–53.” Gaithersburg, MD, August 2009. http://purl.access.gpo.gov/GPO/LPS117689.

———. “FIPS 140-1 and FIPS 140-2 Vendor List.” 2012. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

National Vulnerability Database. “NVD’s CVE and CCE Statistics Query Page.” 2011. http://nvd.nist.gov/statistics.cfm.

Nelson, John. *The Operational Impacts of the Global Network Enterprise Construct*. United States Army Command and General Staff College, Fort Leavenworth, KS, 2010.

Office of Management and Budget. *Guidelines and Discount Rate for Benefit-Cost Analysis of Federal Programs*. Circular No. A-94, April 29, 1992.

Pfleeger, Charles P., and, Shari Lawrence Pfleeger. *Analyzing Computer Security: A Threat/ Vulnerability / Countermeasure Approach*. Prentice Hall, New Jersey, 2011.

Piore, Adam. “The Secret War.” *Popular Mechanics*, January 2012.

Pisello, Tom. “Is There a Business Case for IT Security?” *Security Management*. 2004. http://www.securitymanagement.com/article/there-business-case-it-security

Quade, E. S. *A History of Cost-Effectiveness*. Santa Monica, CA: The RAND Corporation, April 1971.

Quest Software. “Quest Management Xtensions – Configuration Manager.” 2011. http://www.quest.com/quest-management-xtensions-device-management-CM/.

Rashid, Fahmida Y. “Adobe Zero-Day Exploit Targeted Defense Contractors.” *eWEEK*. December 2011. http://www.eweek.com/c/a/Security/Adobe-ZeroDay-Exploit-Targeted-Defense-Contractors-383203/.

Reagan, Ronald. U.S. President. Executive Order no. 12291. *Federal Regulation*. National Archives and Records Administration Federal Register. February 17, 1981.

Richardson, Robert. “2009 Computer Crime and Security Survey.” *Computer Security Institute*. 2009. http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf.

———. “2010/2011 CSI Computer Crime and Security Survey.” *Computer Security Institute*. 2011. http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html.

Rosenberg, Barry. “NETCOM, GNEC Directives Transform Army LandWarNet - Defense Systems.” *Defense Systems*. November 13, 2009. http://defensesystems.com/articles/2009/11/18/c4isr-lawrence-army-network-enterprise-technology-command.aspx.

Ross, Jeanne W., Peter Weill, and David Robertson. *Enterprise Architecture as Strategy: Creating a Foundation for Business Execution*. Boston, Mass: Harvard Business School Press, 2006.

SANS. “Top Cyber Security Risks – Executive Summary.” September 2009. http://www.sans.org/top-cyber-security-risks/summary.php.

———. “Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines.” August 10, 2009. http://www.sans.org/critical-security-controls/.

Schnackenburg, Paul. “Microsoft System Center: The New Look of SCCM.” *Microsoft TechNet Magazine.* March 2011. http://technet.microsoft.com/en-us/magazine/gg675930.aspx.

Seffers, George L. “Improved Cloud over the Horizon for Warfighters.” *Signal Online*. November 10, 2011. http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2795&zoneid=333.

Shavlik. “Case Study: Harbor One Credit Union.” *Shavlik Technologies*. 2011. http://www.shavlik.com/assets/docs/cs-harborone-credit-union.pdf.

Sheftick, Gary, and Delawese Fulton. “Army Migrating to Vista.” *Army News Service.* May 20, 2009. http://www.army.mil/article/21389/army-migrating-computers-to-vista/.

Shostack, Adam. “Quantifying Patch Management.” *Secure Business Quarterly*. 2003. http://www.homeport.org/~adam/sbq_patch_ashostack.pdf.

Snyder, Derek J. “Design Requirements for Weaponizing Man-Portable UAS in Support of Counter-Sniper Operations.” Master’s thesis, Naval Postgraduate School, 2011.

Snyder, P. A. “The Department of Defense Must Combat Terrorism with Cyber Attacks.” *Defense Technical Information Center*. October 20, 2008. http://handle.dtic.mil/100.2/ADA500190.

Symantec. “Altiris 7.0 Planning and Implementation Guide Version 1.2.” 2011. http://www.symantec.com/business/support/resources/sites/BUSINESS/content/live/HOW_TO/9000/HOWTO9811/en_US/Altiris%207%20Planning%20%20Implementation%20Guide%20-%20v1%202.pdf.

———. “Altiris Client Management Suite 7.1 from Symantec.” 2011. http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-client_management_suite_7_1_DS_21178300.en-us.pdf.

———. “Altiris Patch Management Solution for Windows 7.1 from Symantec User Guide.” 2011. http://www.symantec.com/business/support/resources/sites/BUSINESS/content/live/DOCUMENTATION/3000/DOC3505/en_US/PatchWindows_user_guide.pdf. 2011.

Terpy, John F. “An Investigation of Network Enterprise Risk Management Techniques to Support Military Net-Centric Operations.” Master’s thesis, Naval Postgraduate School, 2009.

Thompson, Martin. “Microsoft SCCM (ConfigMgr) Plug-is Group Test.” *The ITAM Review*. February, 2012. http://www.itassetmanagement.net/microsoft-configmgr-plugins/.

U.S. Army Network Enterprise Technology Command. “ConfigMgr 2007 Enterprise Architecture: SysMan.*” NETCOM*. January 26, 2009.

———. “NetOps Implementation Update: SCCVI Employment (eEye Retina / Remote Enterprise Manager).” Proceedings from the LandWarNet Conference, *Armed Forces Communications and Electronics Organization.* Tampa, FL, 2008. www.afcea.org/events/pastevents/documents/SCCVIUpdateBrief.ppt.

———. “Tier 2 & 3 (Child Site) Build Guide: SysMan ConfigMgr 2007.” *NETCOM*. 2008.

U.S. Department of Homeland Security. “Fact Sheet: Protecting Our Federal Networks Against Cyber Attacks.” April 8, 2008. https://www.hsdl.org/?view&did=486707.

———. “Significant Cyber Incidents Since 2006.” January 19, 2012. https://www.hsdl.org/?view&did=12410.

U.S. Government Accountability Office. *Agencies Face Challenges in Implementing Effective Software Patch Management Processes*, by Robert F. Dacey. (GAO-04-816T). Washington, DC: GPO, 2004. http://www.gao.gov/new.items/d04816t.pdf.

———. *CYBERCRIME: Public and Private Entities Face Challenges in Addressing Cyber Threats*, by Dave Powner. (GAO-07-705). Washington, DC: GPO, 2007. http://www.gao.gov/assets/270/262608.pdf.

———. *Department of Defense Cyber Efforts: DoD Faces Challenges in its Cyber Activities*, by Davi M. D'Agostino. (GAO-11-75). Washington, DC: GPO, 2011. http://www.gao.gov/new.items/d1175.pdf.

———. *DoD's Standard Procurement System: Continued Investment Has Yet to be Justified*, by Joel C. Willemssen. (GAO-02-392T). Washington, DC: GPO, 2002, http://www.gao.gov/new.items/d02392t.pdf.

———. *Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, by Robert F. Dacey. (GAO-03-1138T). Washington, DC: GPO, 2003. http://www.gao.gov/new.items/d031138t.pdf.

U.S. Library of Congress. Congressional Research Service. *The Economic Impact of Cyber-Attacks*, by Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, CRS Report RL32331. Washington, DC: Office of Congressional Information and Publishing April 1, 2004. http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

U.S. Secretary of Defense. Information Assurance Workforce Improvement Program (DOD 8570.1M). Washington, DC: Department of Defense. 2005. http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.

United States Cyber Command. *Wikipedia, the Free Encyclopedia*. February 17, 2012. http://en.wikipedia.org/wiki/United_States_Cyber_Command.

Vieth, Warren. "Rumsfeld, Army Chief at Odds on Weapon System." *Los Angeles Times*. May 17, 2002. http://articles.latimes.com/2002/may/17/nation/na-crusade17.

Wikiquote. "Voltaire." *Wikiquote*. April 24, 2012. http://en.wikiquote.org/wiki/Voltaire.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California